NORMAN

SecuritySuite

Benutzerhandbuch

Version 8.00

SAND BOX | STATIS-TICS | UPDATE | UNREAD MAIL | SECURED | VIRUS SCAN | DOCU-MENTS

- Antivirus
- Antispam
- Intrusion Guard
- Personal Firewall
- Parental Control
- Privacy Tools

NORMAN®

Eingeschränkte Garantie

Norman garantiert, dass die im Lieferumfang enthaltene CD-ROM bzw. DVD sowie die Dokumentation frei von Produktionsfehlern sind. Bei Reklamation eines Fehlers innerhalb von 30 Tagen nach Erwerb des Produkts ersetzt Norman die fehlerhafte CD-ROM bzw. DVD und/oder Dokumentation kostenlos. Jeder Reklamation ist der Kaufbeleg beizufügen.

Diese Garantie beschränkt sich auf den Austausch des Produkts. Norman übernimmt keinerlei Haftung für jegliche andere Art von Verlusten oder Schäden, die durch die Verwendung der Software oder der Dokumentation oder durch darin enthaltene Fehler oder mangelnde Informationen entstehen, einschließlich, aber nicht beschränkt auf Ertragsverluste.

Hinsichtlich Fehlern oder Mängeln der CD-ROM, DVD, der Dokumentation oder dieser Lizenzvereinbarung setzt diese Garantie jegliche anderen ausdrücklichen oder implizierten Garantien außer Kraft, u. a. die implizierte Garantie bezüglich der Marktfähigkeit und Eignung für bestimmte Zwecke.

Insbesondere übernimmt Norman ungeachtet der durch die Lizenzvereinbarung auferlegten Einschränkungen hinsichtlich jeglicher speziellen Verwendung oder Einsatzzwecke keinerlei Haftung im Falle von Ertragsverlusten oder anderer kommerzieller Schäden, u. a. auch keinen Schadenersatz für Aufwendungen bei Vertragserfüllung oder Folgeschäden.

Diese Garantie läuft 30 Tage nach Erwerb des Produkts ab.

Die im vorliegenden Dokument enthaltenen Informationen sowie die Funktionalität der Software kann ohne Ankündigung geändert werden. Die Software darf gemäß den Bedingungen der Lizenzvereinbarung verwendet werden. Der Käufer darf zu Sicherungszwecken eine Kopie der Software erstellen. Kein Teil dieser Dokumentation darf zu irgendeinem anderen Zweck als der persönlichen Verwendung durch den Käufer ohne ausdrückliche schriftliche Genehmigung von Norman in irgendeiner Form oder mit irgendwelchen Mitteln, sei es elektronisch oder mechanisch, einschließlich der Erstellung von Fotokopien oder Aufzeichnungen oder der Verwendung von Systemen zur Datenspeicherung und -abrufung, reproduziert oder übertragen werden.

Das Norman-Logo ist eine eingetragene Marke von Norman ASA.

In dieser Dokumentation erwähnte Produktnamen sind entweder Marken oder eingetragene Marken des jeweiligen Eigentümers. Sie werden lediglich zu Identifizierungszwecken angegeben.

Die Norman-Dokumentation und -Software unterliegen dem

Copyright © 1990-2010 Norman ASA.

Alle Rechte vorbehalten.

Überarbeitet im März 2010.

Einführung 4
Systemvoraussetzungen 4
Informationen zu dieser Version 4
Informationen zu diesem Handbuch 4
Schulungen und technische Unterstützung 4
Was ist die Norman Security Suite? 5
Antivirus & Antispyware 5
Personal Firewall 6
Antispam 7
Parental Control 7
Privacy Tools 7
Intrusion Guard 8

Installation 9
Abrufen der Software 9
Lizenzschlüssel 10
Installation läuft 10
Assistenten 12
Installationsassistent 12

Erste Schritte 13
Anwendungssymbol in der Taskleiste 13
Warnsymbole in der Taskleiste 14
Öffnen der Anwendung 15
Produktwarnsymbole 15
Einstellungen der Security Suite 15

Startseite 16
Alle Produkte aktualisieren 16
Automatische Updates sind ein- bzw. ausgeschaltet. . 16

Antivirus & Antispyware 17
Hauptseite 17
Quarantäne 18
Dateien in Quarantäne behalten 18
Dateien in Quarantäne 19
Aufgaben-Editor 19
Eine Aufgabe erstellen 20
Geplante Überprüfung erstellen 21
Ausschlussliste 21
Einstellungen 22
Manueller Scanner 25
Internet Protection 26
Weitere Prüfverfahren 29

Personal Firewall 31
Hauptseite 31
Werkzeuge für Fortgeschrittene 33
Regelassistent 33
Dienstprogramm für Echtzeitprotokoll 36
Erweiterte Port-Anzeige 37
Personal Firewall-Regeln exportieren 38
Personal Firewall-Regeln importieren 38
Einstellungen 39
Personal Firewall konfigurieren 39
Erweiterte Einstellungen 39

Antispam 40
Hauptseite 40
Sperren/Zulassen 42
E-Mail-Adresse hinzufügen/entfernen 42
Einstellungen 43
Filtergenauigkeit 43
Spamkontrolle konfigurieren 43

Parental Control 44
Hauptseite 45
Benutzerkonfiguration 46
Standardprofileinstellungen 47
Benutzer anlegen 48
Protokollanzeige 50
Einstellungen 50

Privacy Tools 51
Programmverlauf eines Benutzers löschen 51
Sicher löschen 52

Intrusion Guard 53
Hauptseite 53
Einstellungen 53
Treiber und Speicher 54
Prozesse 55
Netzwerk 56

Installieren und aktualisieren 57
Hauptseite 57
Einstellungen 58
Aktualisierungsmethode auswählen 58
Proxy-Einstellungen 59

Support Center 60
Hauptseite 60
Hilfe und Fehlerbehebung 60
Kontakt 60
Automatische Reparatur 61
Protokollanzeige 61

NSS deinstallieren 62

Anhang A 63
Was ist eine Sandbox? 63

Anhang B 64
Advanced System Reporter 64
Betriebssystemintern 65
Internet Explorer 66
Prozesse 67

Copyright © 1990-2010 Norman ASA

Einführung

Systemvoraussetzungen

Diese Version unterstützt die Installation der Norman Security Suite, Version 8.00 auf Computern mit den Betriebssystemen Windows XP, Windows Vista und Windows 7 entsprechend den folgenden Spezifikationen:

Windows		XP	Vista	7
Antivirus		☑	☑	☑
Intrusion Guard		nur 32 Bit	☑	☑
Personal Firewall			☑	☑
Parental Control			☑	☑
Antispam [1)]			☑	☑
Privacy Tools			☑	☑
Service Pack	oder höher	2	1	
Prozessor (Pentium-basiert)	Empfohlen	1,8 GHz		
RAM	Empfohlen	2 GB		
Internet Explorer	oder höher	7 (8)		
Freier Speicherplatz auf Festplatte	Empfohlen	500 MB		
Bildschirmauflösung	Empfohlen	1024x768		

[1)] Antispam ist nur für Windows Outlook, Outlook Express und Vista Mail verfügbar.

Informationen zu dieser Version

Das aktuelle Release steht in mehreren Sprachen zur Verfügung. Es wird in unregelmäßigen Abständen um neue Sprachen erweitert. Wenden Sie sich an Ihren Norman-Vertragshändler, wenn Sie Informationen zur Security Suite in Ihrer Sprache benötigen. Detaillierte Informationen hierzu finden Sie auf der Website von Norman. Sie können sich aber auch an Ihren lokalen Händler wenden, wenn Sie weitere Informationen zu Sprachversionen wünschen.

Informationen zu diesem Handbuch

In diesem Handbuch werden Produkte, Merkmale und Hauptfunktionen der Norman Security Suite im Überblick dargestellt. Eine ausführliche Beschreibung aller verfügbaren Optionen finden Sie in der Onlinehilfe.

HINWEIS: Besondere oder wichtige Hinweise sind mit einem Ausrufezeichen am linken Rand gekennzeichnet.

Schulungen und technische Unterstützung

Mit Anfragen zu Schulungen und technischer Unterstützung wenden Sie sich bitte an Ihren Händler vor Ort oder an Norman ASA. Norman bietet technische Unterstützung und Beratung zur Security Suite und zu allgemeinen Sicherheitsfragen an. Die technische Unterstützung beinhaltet zudem die Gewährleistung der Qualität Ihrer Antivireninstallation, einschließlich Unterstützung bei der Anpassung der Security Suite an Ihre Anforderungen. Beachten Sie, dass der Umfang der angebotenen Dienstleistungen je nach Land variiert.

Kontaktangaben zu Niederlassungen von Norman finden Sie auf der letzten Seite des Handbuchs.

Copyright © 1990-2010 Norman ASA

Was ist die Norman Security Suite?

Die Norman Security Suite (NSS) ist ein Softwaresicherheitspaket, das sich aus sechs verschiedenen Sicherheitsanwendungen zusammensetzt:

☑ **Antivirus & Antispyware**	Verhindert das Eindringen von Viren in den Computer
☑ **Personal Firewall**	Verhindert den Missbrauch Ihres Computers als Transit für unerwünschten Datenverkehr durch Hacker
☑ **Antispam**	Blockiert unerwünschte und Massen-E-Mails
☑ **Parental Control**	Verhindert den Besuch von Kindern auf Websites mit ungeeigneten Inhalten
☑ **Privacy Tools**	Sorgt für sicheres Löschen von Dateien und persönlichen Daten.
☑ **Intrusion Guard**	Verhindert das Eindringen bösartiger Programme in Ihren Computer

* Die beiden letzten Anwendungen – Privacy Tools und Intrusion Guard – sind nur in der Version Security Suite PRO enthalten.

Die Norman Security Suite ist nach der Installation sofort einsatzbereit. Die standardmäßigen Konfigurationseinstellungen bieten den benötigten Schutz. Sie müssen sich nicht durch sämtliche Konfigurationsoptionen kämpfen, um das Programm zum Laufen zu bringen. Dennoch ist es hilfreich, eine Vorstellung davon zu haben, wie das Programm funktioniert, und sich mit den Grundfunktionen vertraut zu machen. In diesem Handbuch wird auf bestimmte hilfreiche Funktionen hingewiesen, und es werden Tipps gegeben, mit deren Hilfe sich das Programm optimal einsetzen lässt.

HINWEIS: Vor der Verwendung der Personal Firewall müssen Sie einen Assistenten ausführen. Nähere Informationen finden Sie im Abschnitt „Installationsassistent“ auf Seite 12.

Antivirus & Antispyware

Dieses Virenschutzprogramm scannt Ihren PC auf Schadsoftware (Malware). Bei Malware handelt es sich um Computerviren, -würmer, Trojaner und sonstige unerwünschte Codes. Spyware entfaltet keine zerstörerische Wirkung wie herkömmliche Viren. Die unerwünschte Offenlegung persönlicher Daten kann jedoch ebenso großen Schaden anrichten. Die einzigarte Sandbox von Norman bietet proaktiven Schutz –und das sogar vor unbekannten Viren.

Weitere Informationen zur Sandbox finden Sie auf Seite „Anhang A“ auf Seite 63.

Viren lassen sich automatisch von Festplatten, Wechselmedien, aus E-Mail-Anhängen usw. entfernen. Die Antiviren- und Antispyware-Anwendung prüft Dateien beim Öffnen und entfernt möglicherweise vorhandene Viren automatisch. Die Security Suite beinhaltet zwei Hauptscanner – den automatischen Scanner und den manuellen Scanner – sowie diverse andere Scanverfahren.

Wir empfehlen, den Computer gelegentlich auch manuell zu prüfen. Über das Taskleistenmenü können Sie den gesamten Computer überprüfen lassen – und zwar spontan. Ferner können Sie mithilfe des Kontextmenüs beim Durchsuchen von Ordnern einzelne Dateien prüfen oder Normans Bildschirmschoner aktivieren, wodurch ebenfalls eine Virenüberprüfung in Gang gesetzt wird. Wenn Sie die Arbeit fortsetzen, wird die Prüfung abgebrochen und bei der nächsten Aktivierung des Bildschirmschoners an derselben Stelle wieder aufgenommen. Regelmäßige manuelle Prüfungen können Sie mit dem Aufgaben-Editor und Zeitplaner einrichten. Dort können Sie auch festlegen, welcher Bereich des Computers wann geprüft werden soll.

Dieses Produkt wird mit vorkonfigurierten Einstellungen geliefert, die ausreichen sollten, um Ihren Computer vor Virenangriffen zu schützen. Die Module können Sie jedoch so konfigurieren, dass die jeweilige Anwendung Ihren individuellen Anforderungen genügt.

Copyright © 1990-2010 Norman ASA

Personal Firewall

Immer wenn Sie mit dem Internet verbunden sind, E-Mails lesen oder im Web surfen, stellen Sie Verbindungen zu Computern auf der ganzen Welt her – und diese zu Ihnen. Und da fangen die Probleme an. Wenn Hacker in Ihren Computer eindringen, können sie auf Ihre privaten Dokumente zugreifen, Ihren Computer für ihre eigenen Zwecke missbrauchen oder ihn sogar völlig nutzlos machen, indem sie wichtige Systemdateien löschen.

Die vorliegende Anwendung dient in erster Linie dem Schutz vor Hackerangriffen und kontrolliert daher den eingehenden und ausgehenden Datenverkehr Ihres Computers gemäß einer Sicherheitsrichtlinie (einem Regelsatz). Diese Regeln werden (automatisch oder benutzerspezifisch) beim Installieren des Produkts festgelegt.

Der Regelassistent der Anwendung kann automatisch Regeln für den Internetzugriff der Anwendung erstellen. Es gibt unterschiedliche Modi für erfahrene und unerfahrene Benutzer, und die Anwendung kann sogar den Servermodus erkennen. Zudem können Sie Regeln erstellen und ändern sowie Details zum Datenverkehr und der Aktivität der Ports anzeigen.

Daneben bietet die erweiterte Personal Firewall folgende Funktionen:

- **Startschutz (Launcher Protection),**
  - der Versuche einer Anwendung erkennt, sich selbst über eine andere Anwendung zu starten.
- **Schutz vor getarnten Starts (Stealth Launch Protection),**
  - der bösartige Anwendungen enttarnt, die versuchen, über andere Anwendungen auf das Internet zuzugreifen. Die Personal Firewall verfolgt alle übergeordneten Anwendungen.
- **Schutz vor dem Missbrauch von Prozessen (Process Hijacking Protection),**
  - der verhindert, dass bösartige Anwendungen einen „vertrauenswürdigen“ Prozess für das Einschleusen von DLL-Dateien oder Threads übernehmen.
- **Volltarnmodus (Full Stealth Mode),**
  - der sicherstellt, dass alle Ports Ihres Computers von außen unsichtbar sind.
- **Erweiterte svchost-Verwaltung,**
  - bei der für jeden svchost-Dienst gesonderte Regeln gelten statt einer allgemeinen Regel für die Gruppe von Diensten, die in jeder Sitzung der svchost.exe enthalten sein kann.
  - **Svchost** ist ein generischer Hostprozess für Dienste unter Windows 2000/XP/2003/Vista, der für die ordnungsgemäße Ausführung diverser Netzwerk- und Internetprozesse erforderlich ist. Dieser Dienst kann viele Instanzen gleichzeitig ausführen, die jeweils für den Betrieb der einzelnen Computer notwendig sind. Der Dienst ist berechtigt, häufig auf das Internet zuzugreifen, und wird wie jede andere Anwendung, die sich mit dem Internet verbindet, von der Firewall überwacht. Diese gibt bei verdächtigen Aktivitäten eine Warnung aus. Während viele Firewalls nur über eine einzige allgemeine Regel für den Umgang mit svchost verfügen, die sich noch dazu meist nicht bearbeiten lässt, unterscheidet diese Firewall zwischen unterschiedlichen Instanzen und erkennt, ob der Prozess bekannt oder unbekannt ist. Daneben finden sich in den Hilfedateien der Anwendungen Konfigurationsoptionen für eine Reihe von svchost-Diensten.
- **Pharming-Schutz,**
  - der durch den Schutz der HOSTS-Datei und die damit einhergehende Ausschaltung der meistverbreiteten Pharming-Angriffsmethode erfolgt.
  - Das Kunstwort **Pharming** ist aus den Begriffen „Phishing“ und „Farming“ zusammengesetzt (im nachstehenden Abschnitt „Antispam“ finden Sie eine Erläuterung des Begriffs „Phishing“). Von Pharming spricht man, wenn Sie beim Aufrufen einer Website durch Hackermanipulation auf eine andere, gefälschte Site umgeleitet werden. Pharming funktioniert so, dass entweder die Datei „HOST“ auf dem Zielcomputer verändert wird oder Schwachstellen in der DNS-Serversoftware ausgenutzt werden. Domänennamenserver (DNS) sind für die Auflösung von Internetnamen in die eigentlichen IP-Adressen zuständig. In den letzten Jahren wurden die Pharming- und Phishing-Methoden häufig zum Diebstahl von Online-Identitätsdaten eingesetzt. Pharming ist zu einem ernsten Problem für eCommerce-Unternehmen und im Onlinebanking geworden. Um dieser Bedrohung wirksam zu begegnen, sind komplexe Antipharming-Maßnahmen erforderlich.

Copyright © 1990-2010 Norman ASA

Antispam

Die Antispam-Anwendung schützt vor unerwünschten Werbe- und Massensendungen per E-Mail (sogenannter „Spam“), die u. U. eine Bedrohung für das System darstellen. Antispam blockiert Spam, Phishing-Angriffe und sonstige E-Mail-Bedrohungen, bevor sie Ihren Computer erreichen. Mithilfe von Sperr- und Zulassungslisten können Sie selbst bestimmen, von wem Sie E-Mails annehmen und welche Inhalte zum E-Mail-Client weitergeleitet werden dürfen.

So wie Antiviren-Anwendungen mit Virendefinitionsdateien arbeiten, um Malware zu erkennen, verwenden Antispam-Lösungen Definitionsdateien, um unerwünschte E-Mails herauszufiltern. Virendefinitionsdateien nutzen Virensignaturen, um zu ermitteln, ob eine bestimmte Datei infiziert ist, wohingegen Antispam-Definitionen mithilfe eines bestimmten Kriteriensatzes ermitteln, welche E-Mails vermutlich Spam beinhalten. Spam-Definitionsdateien analysieren E-Mails anhand von Sprache, Bildern, Farben, Hyperlinks, die die Mail enthält, sowie anhand der Absender- und IP-Adresse. Trotzdem lässt sich nicht mit letzter Sicherheit sagen, ob es sich bei einer vorliegenden E-Mail um Spam handelt oder nicht.

- **Spam**
  - Unter Spam versteht man unerwünschte E-Mail, normalerweise Produktwerbung. Spam ist meist harmlos, kann aber lästig und zeitraubend sein.
- **Phishing**
  - Als Phishing bezeichnet man das Versenden von E-Mail unter dem Vorwand, ein seriöses öffentliches oder privates Unternehmen zu sein, um Privatinformationen zu erschleichen und somit Identitätsdaten zu stehlen. In solchen E-Mails werden Sie beispielsweise aufgefordert, persönliche Informationen wie Kreditkarten- oder Kontonummern zu aktualisieren, also Informationen, die den echten Unternehmen längst vorliegen. Die Websites sind nachgestellt, sehen aber oft täuschend echt aus und dienen ausschließlich dem Zweck, Daten zu stehlen. Der Begriff „Phishing“ selbst ist vom englischen Wort für „Fischen“ abgeleitet und bemüht das Bild von Köder und Haken, denen der Empfänger solcher Angriffe gleichsam zum Opfer fällt.

Parental Control

Das Internet ist nicht unbedingt ein sicherer Ort. Zudem gibt es Websites, die Kinder lieber nicht zu sehen bekommen sollten. Sofern wir das Surfverhalten unserer Kinder und Teenager nicht ständig überwachen, besteht die Möglichkeit, dass diese gewollt oder ungewollt Websites mit gefährlichem oder obszönem Inhalt aufrufen.

Mit dem Kinder- und Jugendschutz können Sie den Zugang zu Websites bestimmter Kategorien unterbinden und sogar alle Sites blockieren, die Sie nicht ausdrücklich genehmigt haben. Darüber hinaus können Sie die Zeit beschränken, die ein Benutzer im Internet surfen darf, und festlegen, zu welchen Tageszeiten dies erlaubt ist.

Kurz gesagt können Sie auf der Basis des Alters oder anderer zu berücksichtigender Kriterien für den einzelnen Benutzer ein persönliches Nutzungsprofil anlegen.

Privacy Tools

Viele Anwendungen, darunter auch das Betriebssystem selbst, protokollieren Benutzeraktivitäten, also z. B. welche Dateien geöffnet, welche Websites besucht und welche Dokumente aufgerufen wurden. Es handelt sich dabei um einen benutzerfreundlichen Mechanismus, der wiederkehrende Aufgaben bequemer macht, etwa den Besuch der selben Onlinezeitung oder die Weiterbearbeitung einer Textdatei.

So benutzerfreundlich dies sein mag, ergibt sich ein Datenschutzproblem. Andere Benutzer desselben Computers oder Personen, die Ihren Computer zu einem späteren Zeitpunkt prüfen, können Einsicht in diese Protokolldateien nehmen und Dinge entdecken, die möglicherweise vertraulich sind. Auch das Löschen von Dateien entfernt nicht alle Spuren. Fortgeschrittene Tools können gelöschte Dateien wiederherstellen und die Sicherheit sensibler Dokumente gefährden. Protokolle verfolgen Internetsuchen und Dateien, die Sie auf Ihrem Computer öffnen.

Diese Funktion hat enorme Bedeutung für Ihren Datenschutz. Denn sie birgt das Risiko des Social-Engineering und Identitäts- und Kennwortdiebstahls. Die angeeigneten Privatinformationen können wiederum missbraucht werden.

Privacy Tools ermöglichen Ihnen, bestimmte Dateien sicher zu löschen. Die Inhalte solcher Dateien sind dauerhaft gelöscht und lassen sich nicht wiederherstellen. Sie können die Anwendung auch so konfigurieren, dass diverse Protokolldateien mit persönlichen Daten, Cookies und Browserverläufen automatisch gelöscht werden. Das Löschen von Verlaufsprotokollen wirkt sich nicht auf die Einstellungen und Lesezeichen einer Anwendung aus.

Copyright © 1990-2010 Norman ASA

Intrusion Guard

Dies ist ein hostbasiertes Intrusion Prevention System (HIPD), mit dem schädliche Anwendungen davon abgehalten werden, die Kontrolle über Ihren Rechner zu übernehmen. Die Anwendung bietet ein leistungsstarkes Berichtstool und schützt Prozesse, Treiber, Browser und die Hostdatei. Es handelt sich um eine Plattform für proaktiven Thread-Schutz für erfahrene Benutzer.

- Advanced System Reporter-Tool
  - Dieses leistungsstarke Tool ermöglicht Ihnen, installierte Anwendungen, Systemfilter und verdächtige Module zu kontrollieren, die auf Ihrem Computer entdeckt werden.
- Leistungsstarke Echtzeitfunktionen
  - Diese Funktion lässt sich so konfigurieren, dass sie Versuche einzudringen protokolliert, meldet und blockiert.
- Prozessschutz
  - Verhindert, dass schädliche Anwendungen die Kontrolle über andere Anwendungen übernehmen und weitere schädliche Inhalte auf Ihrem Computer installieren.
- Treiberschutz
  - Verhindert das Installieren von Treibern und schützt vor anderen schädlichen Methoden, Low-Level-Zugriff auf Ihr Computersystem zu erlangen.
- Schutz vor Browsermissbrauch
  - Überwacht die Einstellungen Ihres Internet Explorers und verwaltet Cookies. Außerdem ermöglicht dieses Tool das Protokollieren, Melden und Blockieren von Versuchen, Netzwerkfilter zu installieren, z. B. LSP (Layered Service Provider) und BHO (Browser Helper Object).
- Schutz der Datei „HOSTS“
  - Schützt Ihre HOSTS-Datei vor unbefugter Manipulation.

Copyright © 1990-2010 Norman ASA

Installation

Das folgende Kapitel behandelt die Systemanforderungen, den Lizenzschlüssel, das Abrufen des Installationsprogramms und die Installation der Norman Security Suite auf Ihrem Computer.

Abrufen der Software

Beim Kauf der Norman Security Suite ist entweder eine CD mit Installationsprogramm im Lieferumfang enthalten, oder auf Ihrem Kaufbeleg ist ein Hyperlink für den Internetdownload vermerkt.

CD-ROM

Falls Sie eine CD-ROM von Norman erhalten haben, starten Sie damit die Installation.

1. Legen Sie die CD ins CD-ROM-Laufwerk ein.
   - Die CD startet automatisch, und das CD-Menü erscheint. Falls das CD-Menü nach ca. einer Minute noch nicht angezeigt wird, ist die AutoRun-Funktion möglicherweise deaktiviert. Um die CD manuell zu starten, gehen Sie folgendermaßen vor:
     - Durchsuchen Sie den Inhalt der CD, und klicken Sie auf die Root-Datei „Norman.exe“.
     - Klicken Sie nacheinander auf **Start > Ausführen**, und geben Sie „D:\Norman.exe“ ein, wobei Sie den tatsächlichen Laufwerksbuchstaben anstelle von „D“ setzen. Klicken Sie auf **OK**.
2. Wählen Sie die Sprache aus, in der das CD-Menü angezeigt werden soll.
3. Wählen Sie im CD-Menü auf der Seite **Installieren** die Sprache aus, die installiert werden soll.

Der InstallShield-Assistent wird gestartet. Gehen Sie zum Abschnitt „Installation läuft“ auf Seite 10.

Internetdownload

Das Installationsprogramm steht auch als Internetdownload zur Verfügung. Der Internetpfad und das Downloadverfahren sind in Ihren Kaufunterlagen beschrieben. Falls nicht, folgen Sie den nachstehenden Anweisungen, um das Installationsprogramm herunterzuladen und die Installation zu starten.

1. Öffnen Sie den Internetbrowser, und geben Sie die allgemeine Webadresse für Softwaredownloads von Norman ein: **http://www.norman.com/downloads/**
2. Wählen Sie das entsprechende Installationsprogramm der Norman Security Suite für Ihre Sprache aus.

HINWEIS: Achten Sie auf die richtige Auswahl des Installationsprogramms für 64-Bit- bzw. 32-Bit-Computer.

3. Klicken Sie auf **Speichern** oder **Ausführen**.

   a) **Speichern**

   Falls Sie auf **Save** (Speichern) klicken, wird die Datei auf Ihrem Computer gespeichert und die Installation von dort gestartet. Für die Installation vom Computer aus ist keine Internetverbindung erforderlich. Allerdings empfehlen wir, die Internetverbindung auch während der Installation zur Schlüsselvalidierung und Aktualisierung aufrechtzuerhalten.
   - Suchen Sie einen Speicherort für das Installationsprogramm, und klicken Sie auf **Save** (Speichern), um den Vorgang zu bestätigen.
     - Notieren Sie sich den Speicherort des Installationsprogramms.
     - Damit sind Downloadfenster und Browser nicht länger erforderlich und können geschlossen werden.
   - Suchen Sie das Installationsprogramm, und öffnen Sie die Datei mit Doppelklick.
     - Nach erfolgter Installation kann das Installationsprogramm gelöscht werden. Eventuell sollten Sie eine Sicherungskopie erstellen.

   b) **Ausführen**

   Um die Installation direkt vom Internet aus zu starten, klicken Sie auf **Run** (Ausführen). Das Installationsprogramm wird daraufhin heruntergeladen und sofort gestartet. Sollte die Installation fehlschlagen, müssen Sie die Downloadseite erneut aufrufen.

Der InstallShield-Assistent wird gestartet. Gehen Sie zum Abschnitt „Installation läuft“ auf Seite 10.

Copyright © 1990-2010 Norman ASA

Lizenzschlüssel

Mit dem Kauf der Norman Security Suite erhalten Sie einen Produktlizenzschlüssel. Dieser Schlüssel ist für die Aktualisierung des installierten Produkts erforderlich. Antivirenprogramme erfüllen nur dann ihren Zweck, wenn sie regelmäßig aktualisiert werden.

Ich besitze einen Schlüssel

Geben Sie den Schlüssel während der Installation nach Aufforderung durch den InstallShield-Assistenten ein. Dann sucht die Anwendung nach Abschluss der Installation automatisch nach Updates.

Ich besitze keinen Schlüssel

Sie können das Schlüsselfeld auch zunächst freilassen und trotzdem die gesamte Suite installieren. Der Lizenzassistent fordert Sie dann jedoch in regelmäßigen Abständen zur Eingabe eines Schlüssels auf. Eine Aktualisierung des Produkts bzw. der Produkte erfolgt nicht.

Geben Sie nach Abschluss der Installation einen Schlüssel ein

Sie können den Lizenzassistenten der Anwendung starten und den Schlüssel in das vorgesehene Feld eintragen. Nähere Informationen finden Sie im Abschnitt „Lizenzassistent“ auf Seite 58.

Installation läuft

Führen Sie den InstallShield-Assistenten der Norman Security Suite aus (das Installationsprogramm). Wie Sie diesen erhalten, erfahren Sie im Abschnitt „Abrufen der Software“ auf Seite 9. Folgen Sie den Anweisungen auf dem Bildschirm. Um die Installationseinstellungen zu prüfen oder zu ändern, klicken Sie auf **Back** (Zurück).

Der Standardpfad für die Installation lautet `C:\Programme\Norman`.

1. Der Begrüßungsbildschirm des InstallShield-Assistenten erscheint. Klicken Sie auf **Next** (Weiter).
2. Lesen Sie die Lizenzvereinbarung, und akzeptieren Sie diese, um mit der Installation fortzufahren. Klicken Sie auf **Next** (Weiter).
3. Geben Sie einen gültigen Lizenzschlüssel ein. Klicken Sie auf **Next** (Weiter).
   - Der Schlüssel enthält Informationen zu den von Ihnen erworbenen Produkten.
   - Wenn Sie das Produkt nur testen möchten, können Sie dieses Feld freilassen. Wir empfehlen, einen Demoschlüssel einzugeben, um den vollen Funktionsumfang kennenzulernen.

TIPP

KOPIEREN SIE DEN LIZENZSCHLÜSSEL, UND FÜGEN SIE IHN EIN. Wenn ein Exemplar des Lizenzschlüssels in einer E-Mail oder in einem anderen elektronischen Format vorliegt, können Sie den Schlüssel einfach in das Feld für den Lizenzschlüssel kopieren. Dazu markieren Sie ihn und drücken dann **Strg+C**, um ihn zu kopieren. Anschließend setzen Sie den Cursor in das Feld für den Lizenzschlüssel und drücken **Strg+V**, um ihn einzufügen. Achten Sie darauf, dass der Lizenzschlüssel keine Leerzeichen enthält.

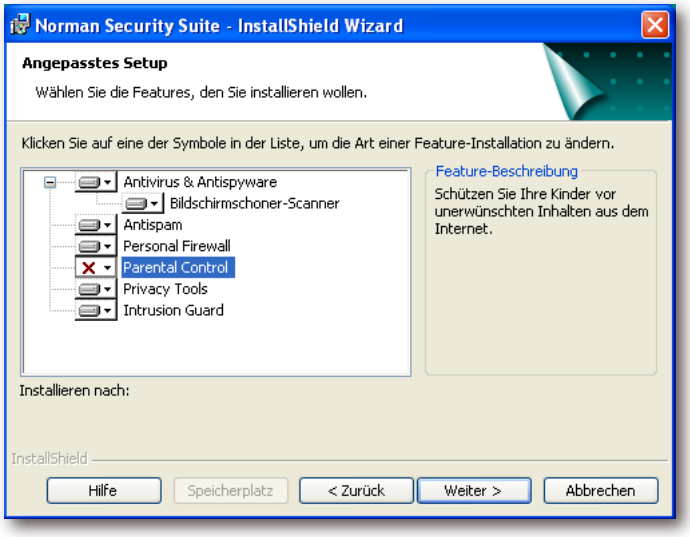
HINWEIS: Wenn Ihnen kein Lizenzschlüssel vorliegt, können Sie das Feld leer lassen und die Suite trotzdem vollständig installieren. Allerdings werden Sie vom Lizenzassistenten in regelmäßigen Abständen zur Eingabe eines Schlüssels aufgefordert. Eine Aktualisierung des Produkts bzw. der Produkte erfolgt nicht. Bei Bedarf hilft Ihnen der Lizenzassistent später beim Erwerb eine Schlüssels.

4. **Das Dialogfeld „Setup Type“ (Setup-Methode)**
   a) Die Option **Complete** (Abschließen) sorgt für die Installation aller Programmfunktionen unter dem Standardpfad.
      - Wählen Sie **Complete** (Abschließen), und klicken Sie auf **Next** (Weiter).
      - Fahren Sie fort mit dem nachstehenden Punkt „7. Bereit zur Installation“.

   b) Wählen Sie **Custom** (Benutzerdefiniert), um zu bestimmen, welche Produkte genau installiert werden sollen, und/oder um einen anderen Speicherpfad festzulegen.
      - Wählen Sie **Custom** (Benutzerdefiniert), und klicken Sie auf **Next** (Weiter).
5. **Custom setup** (Benutzerdefiniertes Setup)
   Die installierbaren Produkte werden als Liste angezeigt.
   - **Antivirus & Antispyware**
     - **Screensaver Scanner**

Copyright © 1990-2010 Norman ASA

- **Antispam**
- **Personal Firewall**
- **Parental Control**
  - Dieses Produkt müssen Sie manuell auswählen, falls es installiert werden soll. Klicken Sie auf das Dropdown-Menü linkerhand und anschließend auf die betreffende Funktion, um sie auf der lokalen Festplatte zu installieren. Die Installation dieses Produkts setzt voraus, dass es von Ihrem Lizenzschlüssel abgedeckt oder Teil Ihrer Testversion ist.
  - Sie können das Produkt nach Wunsch auch später installieren.
- **Privacy Tools**
- **Intrusion Guard**



- Klicken Sie auf **Space** (Speicherplatz), um zu sehen, wie viel Speicherplatz die ausgewählten Installationen erfordern.
  - Klicken Sie auf **OK**, um zum Dialogfeld **Custom setup** (Benutzerdefiniertes Setup) zurückzukehren.
- Klicken Sie auf **Weiter**, um fortzufahren.

6. **Zielordner**

   a) Klicken Sie auf **Next** (Weiter), wenn die ausgewählten Anwendungen unter dem Standardpfad gespeichert werden sollen.

   b) Klicken Sie auf **Change...** (Ändern), um einen anderen Speicherort festzulegen.
   - Wählen Sie einen Speicherort aus der Dropdown-Liste, erstellen Sie einen neuen Ordner, oder geben Sie den Pfad im Eingabefeld für den Ordnernamen ein.
   - Klicken Sie auf **OK**, um zu bestätigen und zum Zielordner zurückzukehren.
   - Klicken Sie auf **Next** (Weiter).

7. Damit kann die Installation beginnen.
   - Klicken Sie auf **Install** (Installieren), um mit der Installation zu beginnen.
8. Installieren der Norman Security Suite.
   - Ein Dialog erscheint mit der Meldung, dass die Anwendung nun gestartet und die installierten Komponenten installiert werden können. Klicken Sie auf **OK**, um fortzufahren.
9. Ein Dialog meldet, dass der Vorgang abgeschlossen ist. Klicken Sie auf **Finish** (Fertigstellen), um den **InstallShield Wizard** (Assistenten) abzuschließen. Das Installationsprogramm wird noch weitere 5-10 Minuten im Hintergrund ausgeführt.
10. Klicken Sie auf **Restart now** (Jetzt neu starten), wenn Sie zum Neustart des Computers aufgefordert werden. Nach dem Neustart erscheint ein Kundenregistrierungsformular. Gleichzeitig startet – sofern die Personal Firewall installiert wurde – der Personal Firewall-Installationsassistent.
    - **Kundeninformationen**
      - Geben Sie bitte die erforderlichen Angaben ein, und klicken Sie anschließend auf **Submit** (Abschicken).
    - **Installationsassistent**
      - Nähere Informationen dazu finden Sie im nächsten Abschnitt.

Copyright © 1990-2010 Norman ASA

Assistenten

Die Norman Security Suite verfügt über drei Assistenten. Sie sind für die Installation und Grundkonfiguration der Produkte zuständig.

InstallShield Wizard
Dieser Assistent dient zur Installation der Norman Security Suite. Er wird auch als Installationsprogramm oder Setup-Datei bezeichnet.

Installationsassistent
Dies ist bei der Installation der Personal Firewall von Bedeutung. Sobald die Norman Security Suite samt Personal Firewall installiert ist, wird ein Assistent für das Setup der Personal Firewall gestartet. Nähere Informationen dazu finden Sie im nächsten Abschnitt.

Lizenzassistent
Dieser Assistent verwaltet Ihre gültigen Produktlizenzen. Nähere Informationen finden Sie im Abschnitt „Lizenzassistent“ auf Seite 58.

Installationsassistent

Nach erfolgter Installation der Norman Security Suite (siehe „Installation läuft“ auf Seite 10) gehört die Personal Firewall nunmehr zu den installierten Funktionen. Der Installationsassistent wird automatisch gestartet.

Es handelt sich dabei um einen Assistenten, der Grundregeln automatisch erstellt, etwa zur Einrichtung des Zugriffs auf relevante Anwendungen. Aufgabe des Assistenten ist es, Programme zu identifizieren, die legitim auf das Internet zugreifen müssen und können. Auf der Basis dessen werden dann Regeln für diese Anwendungen erstellt. Es wird dringend empfohlen, diesen Installationsassistenten auszuführen. Automatisch erzeugte Regeln können Sie später jederzeit mit dem Regelassistenten ändern.

Wenn Sie auf die Ausführung des Installationsassistenten verzichten, kann es zu Problemen beim Internetzugriff des Computers und bei der Aktualisierung wichtiger Anwendungen kommen. Nähere Informationen finden Sie im Abschnitt „Werkzeuge für Fortgeschrittene“ auf Seite 33.

1. Lesen Sie die Einleitungsseite, und klicken Sie auf **Weiter**.
   Der Installationsassistent bietet unterschiedliche Schritte für erfahrene und unerfahrene Benutzer. Erfahrene Benutzer können bestimmte Details festlegen, wohingegen unerfahrene Benutzer durch die automatischen Konfigurationen geführt werden.
2. Wählen Sie Ihren Erfahrungsstand, und klicken Sie auf **Weiter**.

   Unerfahrene Benutzer
   - Angenommen, Sie sind ein durchschnittlicher Internetnutzer ohne Computerfachkenntnisse. In diesem Fall nimmt Ihnen die Firewall die Entscheidungen ab und erfordert Ihrerseits nur minimale Interaktion mit dem Programm.
   - Wählen Sie die Sicherheitsstufe für den Umgang mit Internetverbindungen aus, die auf Ihren Computer (eingehend) oder auf das Internet zuzugreifen versuchen (ausgehend).
     - **Einfacher Modus**.
       - Jede Art von Datenverkehr ist zulässig, sofern keine permanente Regel die Verbindung sperrt. Vor eingehenden Angriffen sind Sie geschützt.
     - **Normaler Modus**.
       - Bei unbekanntem Datenverkehr werden Sie aufgefordert, den Zugriff zuzulassen oder zu verweigern, sofern er nicht von einer permanenten Regel verhindert wird. Sie sind vor eingehenden Angriffen und unerwünschten Anwendungen, die Daten von Ihrem Computer versenden, sicher.

   Erfahrene Benutzer
   - Angenommen, Sie sind mit dem allgemeinen Setup von Firewalls vertraut und wissen, was man unter IP-Adresse und Portnummer versteht. In diesem Fall bietet die Firewall erweiterte Optionen während der Installation und im Betrieb.
3. Folgen Sie den Bildschirmanweisungen in Bezug auf das Hinzufügen weiterer Webbrowser oder E-Mail-Clients, das Konfigurieren von Netzwerkressourcen (erweiterte Konfiguration bei erfahrenen Benutzern) und das Zulassen weiterer bekannter Anwendungen.
4. Klicken Sie schließlich auf **Fertig stellen**, um den Assistenten zu schließen.

Copyright © 1990-2010 Norman ASA

Erste Schritte

Anwendungssymbol in der Taskleiste

Während des Setups wird in der Taskleiste (am rechten unteren Bildschirmrand) ein Symbol platziert. Dieses Symbol bestätigt, dass die Security Suite auf dem Computer installiert ist.

Mit einem Rechtsklick auf das Symbol rufen Sie das Taskleistenmenü der Security Suite auf.

Die Einträge in der Liste mit einem vorangestellten Symbol entsprechen den Einträgen, die im Menü **Start > Programme > Norman Security Suite** enthalten sind. Das Menü dient als Verknüpfung zu den Hauptmodulen der Norman Security Suite sowie zu bestimmten typischen Aufgaben.

- **Internet Update**
  - Aktivieren Sie die Funktion „Internet Update“, um die installierten Produkte zu aktualisieren.
- **Norman Security Suite**
  - Öffnen Sie die Anwendung „Norman Security Suite“.
- **Personal Firewall aktivieren (deaktivieren)**
  - Wechselt zwischen aktiviertem und deaktiviertem Status der Personal Firewall.
- **Computer prüfen**
  - Hiermit starten Sie eine manuelle Prüfung des gesamten Computers.
- **Automatischen Scanner anhalten (starten)**
  - Wechselt zwischen aktiviertem und deaktiviertem Status der automatischen Prüfung.
- **Update-Status...**
  - Hier wird der Update-Status... für installierte Produkte angezeigt. Diese Funktion ist auch der Ausgangspunkt für Meldungen bezüglich veralteter Virendefinitionsdateien, abgelaufener Lizenzvereinbarungen und anderer Informationen.

HINWEIS: Welche Menüoptionen verfügbar sind, hängt von den jeweils installierten Produkten ab. So ist die Option zum Aktivieren bzw. Deaktivieren der Personal Firewall nur sichtbar, sofern diese installiert ist.

Copyright © 1990-2010 Norman ASA

Warnsymbole in der Taskleiste

Das Taskleistensymbol zeigt auch den Status der Security-Suite-Installation an. Gehen Sie mit dem Cursor über das Taskleistensymbol, um Erläuterungen zu Fehler- oder sonstigen Meldungen anzuzeigen.

Roter Kreis

Dieses Symbol bedeutet, dass einige der gegenwärtig ausgeführten Komponenten nicht auf dem neuesten Stand sind. Wenn das Symbol mit einem blinkenden roten Symbol erscheint, gehen Sie mit dem Cursor auf das Symbol, um herauszufinden, welche Komponente aktualisiert werden muss oder ob andere Fehler vorliegen.

HINWEIS: Beim Systemstart wird das rote Symbol so lange angezeigt, bis alle Module gestartet wurden. Je älter und langsamer der Computer ist, desto länger dauert es, bis alle Module geladen wurden. Das normale Norman-Symbol sollte allerdings spätestens nach zwei Minuten erscheinen.

Gelbes Dreieck

Das gelbe Dreieckssymbol, das entweder statisch ist oder blinkt, zeigt an, dass der automatische Scanner manuell deaktiviert wurde, dass die Anwendung neu gestartet werden muss, dass ein Installationsfehler aufgetreten ist oder dass keine aktuellen Definitionsdateien vorliegen.

- **Statisch**
  - Der automatische Scanner wurde manuell in den Einstellungen der Anwendung deaktiviert. Nähere Informationen finden Sie im Abschnitt „Automatischen Scanner aktivieren“ auf Seite 23.
  - Ein Neustart der Anwendung ist erforderlich. Bei einer zurückliegenden Aufforderung zum Neustart wurde möglicherweise die Option **Später neu starten** ausgewählt.
  - Es ist ein Installationsfehler aufgetreten. Versuchen Sie das Problem durch einen Neustart des Computers zu beheben.

- **Blinkend**
  - Die Virendefinitionsdateien sind nicht mehr auf dem neuesten Stand. Das bedeutet, dass sie mindestens zehn Tage alt sind.
  - Der automatische Scanner wurde vom Taskleistenmenü aus angehalten. Gehen Sie mit Rechtsklick auf das Taskleistenmenü. Wählen Sie **Automatischen Scanner starten**.
  - Die Firewall wurde deaktiviert. Gehen Sie mit Rechtsklick auf das Taskleistenmenü. Wählen Sie **Firewall aktivieren**.

Gelbes Zahnrad

Wenn das angezeigte Taskleistensymbol ein Zahnrad trägt, greift der Norman Program Manager gerade auf das Programm zu, vermutlich zu Aktualisierungszwecken. Wir raten Ihnen, den Computer nicht auszuschalten, solange der NPM arbeitet, also solange dieses Symbol sichtbar ist.

HINWEIS: Ein Update sollte höchstens 5-10 Minuten dauern. Falls das Zahnradsymbol länger angezeigt wird, könnte ein Installationsproblem vorliegen. Versuchen Sie in diesem Fall, den Computer neu zu starten. Falls das Zahnrad auch nach erfolgtem Neustart noch angezeigt wird, wenden Sie die Reparaturoption an, die im Abschnitt „„Automatische Reparatur“ auf Seite 61 beschrieben ist.

Symbol des Windows Security Center

Norman ist ein Anbieter von Virenschutzprogrammen, die vom Betriebssystem erkannt werden. Wenn die Virendefinitionsdateien veraltet sind, der automatische Scanner inaktiv ist oder die Firewall deaktiviert wurde, erhalten Sie zudem eine Warnmeldung von Windows. Das Symbol des Security Center wird eingeblendet. Klicken Sie auf das Symbol, um die Windows-Einstellungen anzuzeigen und zu bearbeiten.

Copyright © 1990-2010 Norman ASA

Öffnen der Anwendung

Sie können die Anwendung über das Taskleisten- oder das Windows-Menü aufrufen. Klicken Sie mit der rechten Maustaste auf das Taskleistenmenü, und wählen Sie im Kontextmenü die Option **Norman Security Suite** aus. Klicken Sie im Windows-Menü auf **Start** und dann nacheinander auf **Alle Programme > Norman Security Suite > Norman Security Suite**.

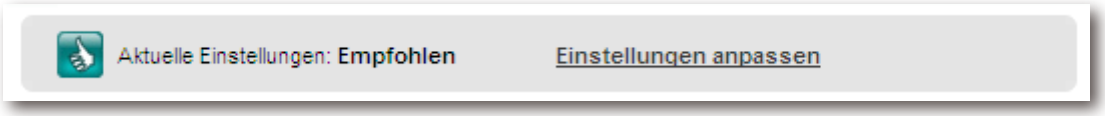
Produktwarnsymbole

Gelegentlich erscheint ein gelbes Dreieck auf dem Menüeintrag der Anwendung. Das kann u. a. bedeuten, dass ein Produkt deaktiviert oder veraltet ist, die Lizenz abgelaufen ist oder eine neu installierte Software endgültig konfiguriert werden muss, um den Installationsvorgang abzuschließen.

HINWEIS: Wenn Sie die Security Suite zum ersten Mal öffnen, erscheint eine Warnmeldung bezüglich der Anwendung Parental Control. Nähere Informationen finden Sie im Abschnitt „Parental Control“ auf Seite 44.

Einstellungen der Security Suite

Diese Anwendung wird mit Standardeinstellungen installiert, und wir empfehlen, diese für den Alltagsbetrieb beizubehalten. In den Hauptseiten der Anwendung können Sie die Option **Einstellungen anpassen** auswählen, um diverse Optionen für die Produkte zu konfigurieren. Achten Sie beim Wechseln zwischen den Einstellungen darauf, wie sich das Symbol verändert und die Bearbeitungstexte der Einstellungen den Platz tauschen.



- Aktuelle Einstellungen: **Empfohlen**
  - Die Standardeinstellungen sind effizient und für den Alltagsbetrieb empfohlen.
  - Um die Standardeinstellungen zu ändern, klicken Sie auf **Einstellungen anpassen**.

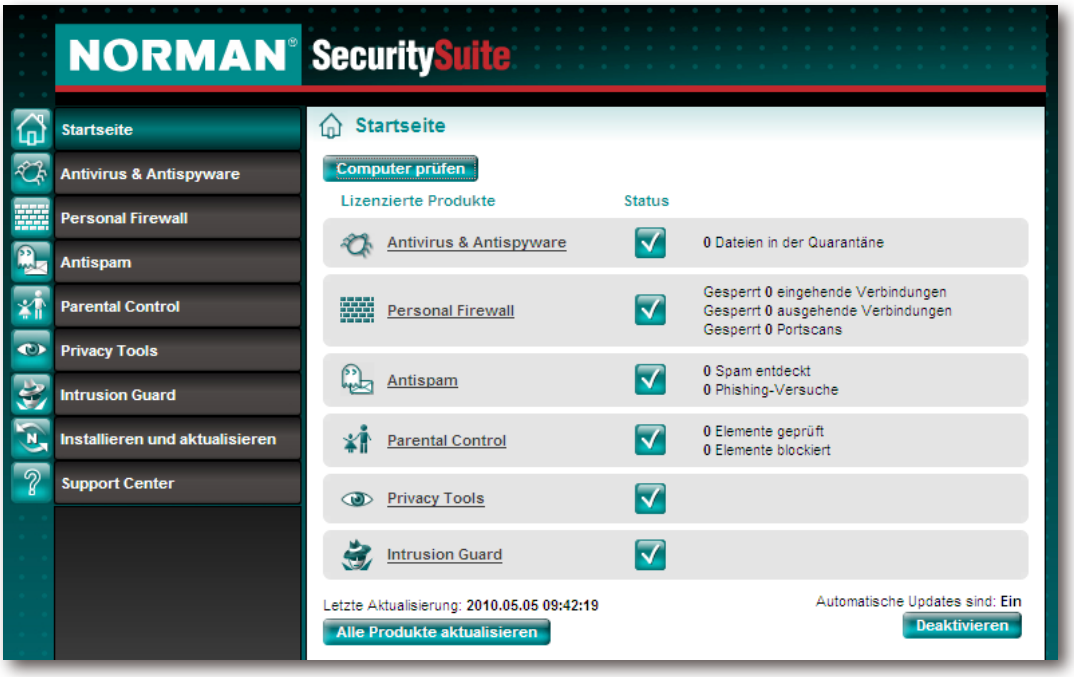
- Aktuelle Einstellungen: **Benutzerspezifisch**
  - Die Benutzereinstellungen lassen sich anpassen bzw. sind angepasst
  - Klicken Sie auf die Option **Empfohlene Einstellungen verwenden**, um sie auf die Standardeinstellungen zurückzusetzen.

HINWEIS: Sie sollten die Standardeinstellungen nur ändern, wenn Ihnen klar ist, wie sich die Änderungen auf das System auswirken. Vergewissern Sie sich, dass die benutzerdefinierten Einstellungen die Sicherheitsstufe nicht herabsetzen. Falls Sie sich nicht sicher sind, sollten Sie bedenken, dass die Standardeinstellungen ausreichenden Schutz bieten.

Copyright © 1990-2010 Norman ASA

Startseite

Öffnen Sie die Anwendung „Security Suite“, um den Status der installierten Produkte anzeigen zu lassen. Näheres zum Öffnen der Anwendung erfahren Sie im Abschnitt „Erste Schritte“ auf Seite 13.



Führen Sie eine Überprüfung des Computers durch, und ermitteln Sie, welche Produkte installiert sind, welchen Status sie haben und welche Detailinformationen zu ihnen vorliegen. Aktualisieren Sie alle Produkte, und klicken Sie auf die automatische Updatefunktion, um sie ein- bzw. auszuschalten.

Um eine manuelle Prüfung des gesamten Computers zu starten, klicken Sie auf **Computer prüfen**. Diese Prüfung verwendet die gleichen Einstellungen wie die des manuellen Scanners. Nähere Informationen finden Sie im Abschnitt „Manueller Scanner“ auf Seite 25.

Lizenzierte Produkte sind diejenigen, die von Ihrem Produktlizenzschlüssel abgedeckt sind. Nähere Informationen finden Sie im Abschnitt „Lizenzschlüssel“ auf Seite 10. Anhand des Statussymbols erkennen Sie, ob die Installation auf dem aktuellen Stand und komplett ist, ob sie aktualisiert werden muss oder ob ein Produkt eventuell noch gar nicht installiert wurde. Die Statistikwerte rechterhand zeigen Daten zu den aktiven Anwendungen an.

HINWEIS: Wenn Sie die Security Suite zum ersten Mal öffnen, erscheint eine Warnmeldung bezüglich der Anwendung Parental Control. Nähere Informationen finden Sie im Abschnitt „Parental Control“ auf Seite 44.

Alle Produkte aktualisieren

Aktualisieren Sie alle installierten Produkte mit einem einfachen Klick. Näheres zu weiteren Einstellungen sowie einen Überblick finden Sie im Abschnitt „Installieren und aktualisieren“ auf Seite 57.

Automatische Updates sind ein- bzw. ausgeschaltet.

Wenn die automatische Updatefunktion aktiviert ist, werden die Produkte regelmäßig aktualisiert. Die Einstellungen können Sie unter „Aktualisierungsmethode auswählen“ auf Seite 58 bearbeiten.

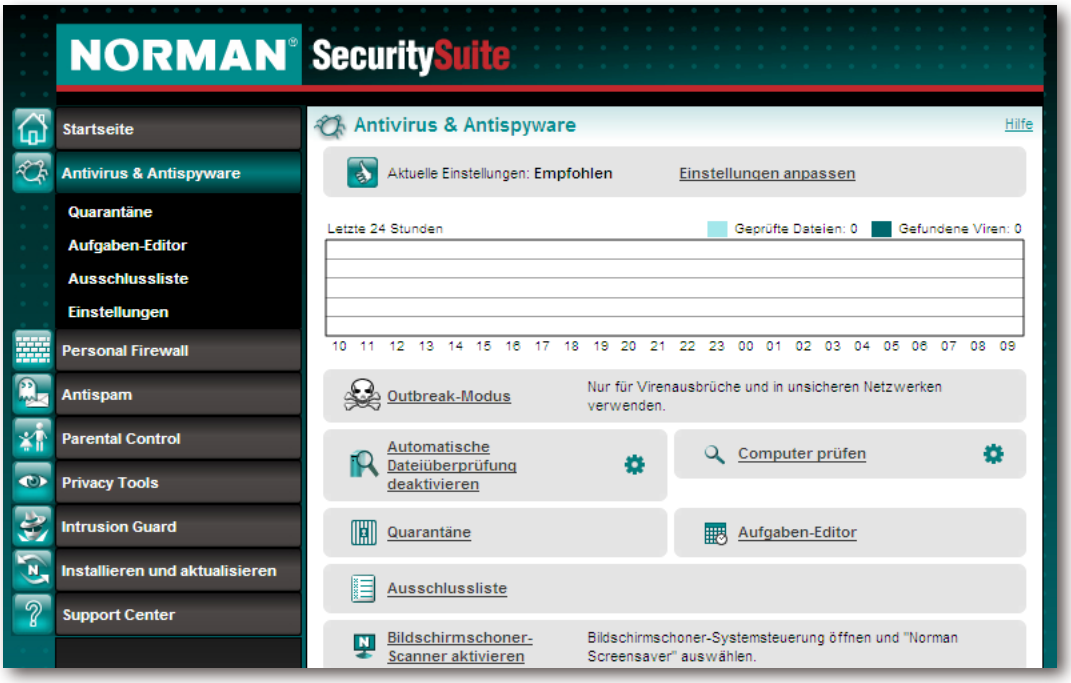
HINWEIS: Es wird dringend empfohlen, die automatische Updatefunktion stets aktiviert zu belassen.

Copyright © 1990-2010 Norman ASA

Antivirus & Antispyware

Öffnen Sie die Anwendung „Security Suite“, und wählen Sie im linken Menü die Option **Antivirus & Antispyware** aus. Nähere Informationen zum Öffnen der Anwendung finden Sie im Abschnitt „Erste Schritte“ auf Seite 13, Informationen zu ihrem Zweck und ihrer Funktionsweise im Abschnitt „Antivirus & Antispyware“ auf Seite 5.

Hauptseite



Diese Antiviren- und Antispyware-Anwendung prüft Ihren PC auf schädliche Software, auch Malware genannt. Das vorliegende Kapitel behandelt die Konfiguration von zwei wichtigen Virenscannern, dem automatischen und dem manuellen Scanner, und zeigt Ihnen ferner, wie Sie Dateien in Quarantäne verwalten, Scans planen und den Bildschirmschoner-Scanner sowie die Antispyware-Funktion aktivieren.

Einstellungen anpassen

Klicken Sie auf diese Option, um die Standardwerte zu bearbeiten. Nähere Informationen finden Sie im Abschnitt „Einstellungen“ auf Seite 22. Allgemeine Informationen zur Wahl zwischen empfohlenen und benutzerdefinierten Einstellungen finden Sie im Abschnitt „Einstellungen der Security Suite“ auf Seite 15.

Scan-Statistik

Die Hauptseite der Anwendung zeigt eine grafische Darstellung der geprüften und der infizierten Dateien der letzten 24 Stunden an. Die statistischen Angaben beziehen sich auf die kombinierten Aktivitäten des manuellen und des automatischen Scanners.

Outbreak-Modus

Dies Funktion sollte nur vorübergehend aktiviert werden im Fall von Virenausbrüchen und beim Verbindungsaufbau zu unbekannten oder unsicheren Drahtlosnetzwerken. Die Aktivierung dieser Option kann sich auf die Leistung und Stabilität des Computers auswirken.

Automatische Dateiüberprüfung deaktivieren

Nähere Informationen finden Sie im Abschnitt **Einstellungen > Automatischer Scanner** auf Seite 23.

Copyright © 1990-2010 Norman ASA

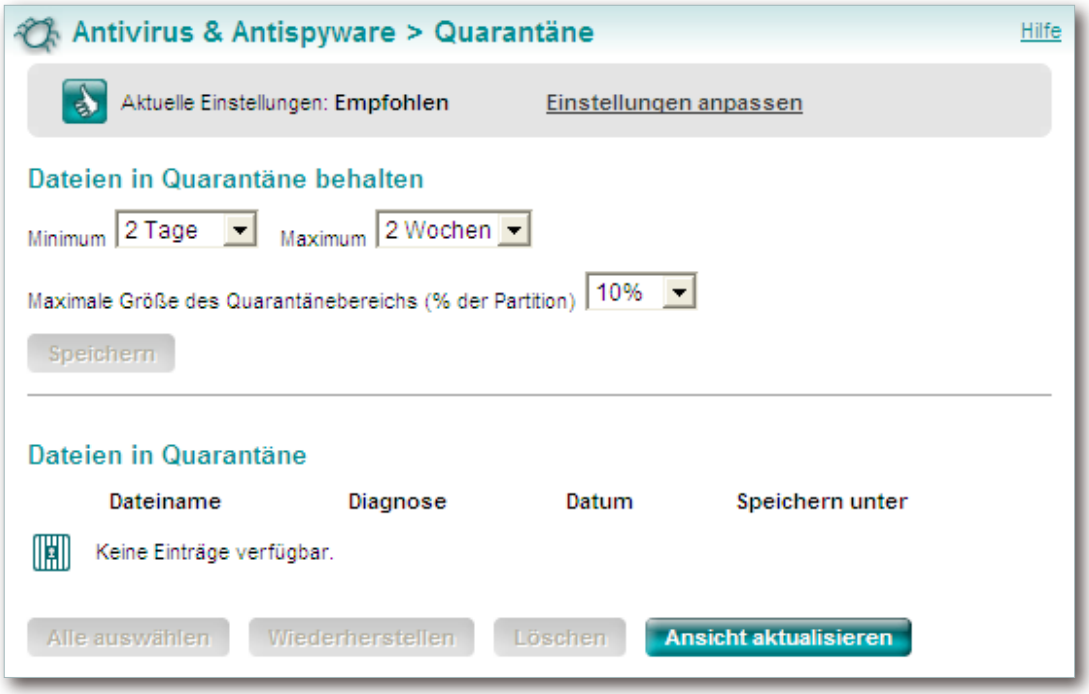
Computer prüfen

Hierbei handelt es sich um den manuellen Scanner, der eine Überprüfung aller Systemlaufwerke vornimmt. Wählen Sie im angezeigten Dialogfeld die Option **Stop**, falls Sie mithilfe der Option **Durchsuchen** einen anderen Bereich prüfen möchten. Klicken Sie auf **Start**, um die manuelle Prüfung fortzusetzen.

Alternativ können Sie diese Prüfung aus dem Taskleistenmenü starten. Klicken Sie mit der rechten Maustaste auf das Symbol der Anwendung in der Taskleiste, und wählen Sie die Option **Computer prüfen** aus.

Informationen zur Konfiguration der manuellen Prüfung finden Sie im Abschnitt „Manueller Scanner“ auf Seite 25.

Quarantäne



Dateien in Quarantäne behalten

Wählen Sie die Option **Einstellungen anpassen**, um das Konfigurationsmenü aufzurufen. Legen Sie die Mindest- und Höchstdauer des Verbleibs von Dateien in Quarantäne und den für sie maximal reservierten Speicherplatz fest.

- **Minimum**
  Legen Sie einen Zeitraum von einem Tag bis zu einer Woche fest. Dateien werden niemals innerhalb der festgelegten Mindestaufbewahrungszeit gelöscht.
- **Maximum**
  Legen Sie einen Zeitraum zwischen einer und vier Wochen fest. Dateien werden nach Überschreiten der Höchstaufbewahrungszeit ohne Vorwarnung gelöscht.
- **Maximale Größe des Quarantänebereichs (% der Partition)**
  Legen Sie fest, wie viel Speicherplatz der aktuellen Partition in Quarantäne befindliche Dateien in Anspruch nehmen dürfen.

HINWEIS: Die maximale Größe kann überschritten werden, falls die in Quarantäne befindlichen Dateien die für sie festgelegte Mindestaufbewahrungszeit noch nicht erreicht haben.

- Klicken Sie auf **Speichern**, um Ihre Änderungen zu bestätigen.

Copyright © 1990-2010 Norman ASA

Dateien in Quarantäne

Infizierte Dateien in Quarantäne sind in einer Liste im Dialogfeld **Dateien in Quarantäne** aufgeführt, sofern Sie das Programm so konfiguriert haben. Das Antivirenprogramm versucht, infizierte Dateien vor dem Löschen und/oder der Überführung in die Quarantäne (je nach Konfiguration) zu reparieren. Dateien in Quarantäne sind entweder infiziert oder wurden durch Internet Protection blockiert.

HINWEIS: Eine Kopie der gelöschten oder blockierten Datei wird standardmäßig in Quarantäne genommen.

Eine Kopie der infizierten und unter Quarantäne gestellten Datei wird gelöscht, es sei denn, sie befindet sich in einem anderen Ordner. In diesem Fall wird sie in Quarantäne verschoben. Wenn der automatische Scanner erkennt, dass `C:\eicar.com` infiziert ist, wird die Datei in Quarantäne genommen. Wenn allerdings der automatische Scanner `C:\Kopie von eicar.com` entdeckt und feststellt, dass diese identisch mit `eicar.com` ist, wird sie nicht in Quarantäne genommen, sondern gelöscht. Wenn `C:\Kopie von eicar.com` sich in `C:\anderer Ordner\` befindet, wird die Datei jedoch aufgrund des neuen Speicherorts in Quarantäne genommen. Dieses Verfahren soll verhindern, dass die Quarantäne überfüllt wird, wenn ein Virus mehrere Kopien derselben Datei in denselben Bereich des Laufwerks geschrieben hat.

Dateien können auch unter Quarantäne gestellt werden, wenn die Antivirenanwendung vermutet, dass sie infiziert sind. In seltenen Fällen kann es auch nach der Aktualisierung der Definitionsdateien vorkommen, dass die Antivirenanwendung feststellt, dass zuvor unter Quarantäne gestellte Dateien doch harmlos sind. Da Typen und Methoden zum Herstellen und Erkennen von Viren sich rasant weiterentwickeln, prüfen Antivirenprogramme die Quarantänedateien nach jedem Update und nach jedem Neustart des Computers.

Falls eine solche Prüfung die Harmlosigkeit einer in Quarantäne befindlichen Datei feststellt, wird diese wiederhergestellt, sofern ein gültiger Dateipfad vorliegt und keine weitere Datei gleichen Namens existiert. Dazu ist kein Benutzereingriff erforderlich, und die mögliche Wiederherstellung einer unter Quarantäne gestellten Datei wird dem Benutzer auch nicht gemeldet.

Aufgaben-Editor

Manchmal ist es von Nutzen, Tasks festzulegen, die mehrmals und/oder in regelmäßigen Abständen ausgeführt werden müssen. Das Überprüfen auf Viren ist ein gutes Beispiel für eine Aufgabe, die regelmäßig ausgeführt werden muss, und der Aufgaben-Editor ist das entsprechende Werkzeug dafür.

Sie können eine Aufgabendatei für Scans erstellen, die wiederholt durchgeführt werden sollen, oder für besondere Scans, die in bestimmten Situationen durchgeführt werden sollen. Wenn Sie beispielsweise Dateien aus dem Internet in dafür vorgesehene Bereiche herunterladen, können Sie eine Aufgabendatei erstellen, die nur diese Bereiche prüft, und die Aufgabe nach dem Herunterladen manuell ausführen. Außerdem können Sie einen Zeitplan für den Task erstellen, damit er zu einer festgelegten Zeit durchgeführt wird.

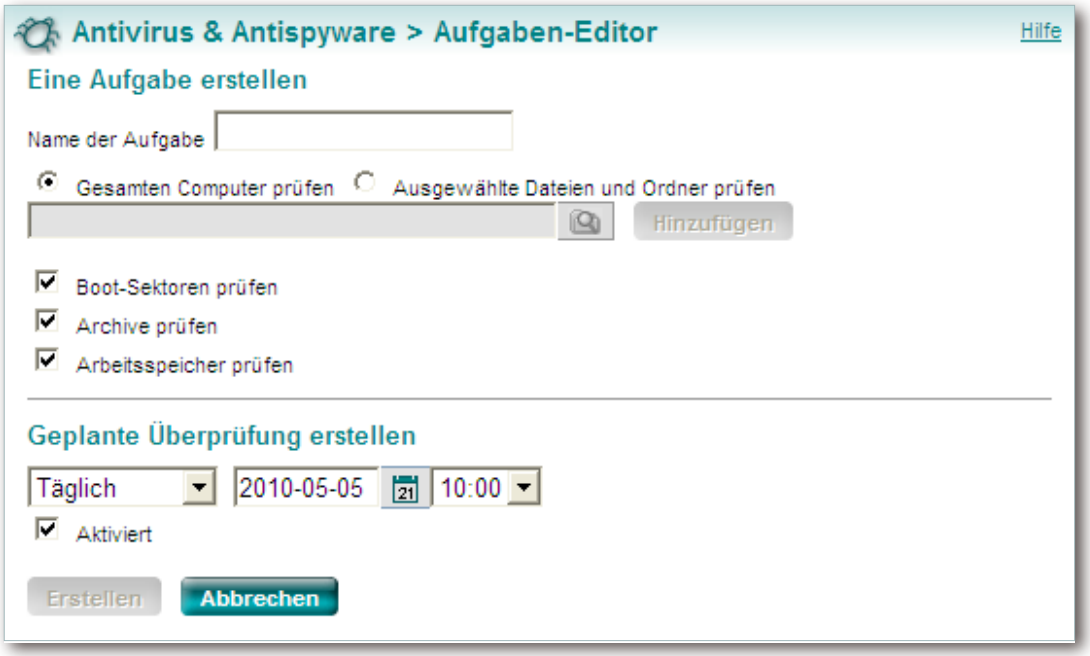
Administratoren können Taskdateien erstellen und an alle Workstations im Netzwerk verteilen, um sicherzustellen, dass Bereiche, die mit besonderer Sorgfalt behandelt werden müssen, regelmäßig überprüft werden.

HINWEIS: Das Dialogfeld Eine Aufgabe erstellen erscheint beim ersten Aufrufen des Aufgaben-Editors oder falls noch keine Aufgaben erstellt wurden.

Alle bestehenden Aufgaben werden als Liste im Dialogfeld „Aufgaben-Editor“ angezeigt.

Copyright © 1990-2010 Norman ASA

Eine Aufgabe erstellen



1. Machen Sie unter **Name der Aufgabe** die entsprechende Angabe.
2. Wählen Sie entweder **Gesamten Computer prüfen** oder **Ausgewählte Dateien und Ordner prüfen**.
   - Klicken Sie auf das Ordnersymbol, um nach Dateien oder Ordnern zu suchen.
     - Hier sind alle Laufwerke in einem Fenster aufgeführt, dessen Funktionen denen des Windows Explorer entsprechen.
     - Klicken Sie auf einen Laufwerksbuchstaben, um nach Verzeichnissen oder Dateien zu suchen.
     - Wenn Sie bestimmte Dateien und Ordner auswählen, sind automatisch alle Unterordner unter dem ausgewählten Laufwerk bzw. Ordner ausgewählt. Sie können die Option für Unterordner, die Sie nicht scannen möchten, deaktivieren.
   - Alternativ können Sie Pfad und Datei oder den Verzeichnisnamen auch direkt in das Eingabefeld eingeben.
     - Der Asterisk (*) wird als Platzhalter akzeptiert, sodass Sie z. B. mit „C:*.*“ das gesamte Laufwerk C: prüfen können.
     - Setzen Sie den Platzhalter am Anfang oder am Ende des Suchbegriffs. Setzen Sie den Platzhalter nicht in der Mitte des Suchbegriffs.
   - Wenn Sie zum Speichern Ihrer Auswahl auf **Hinzufügen** klicken, wird der angegebene Bereich der Aufgabenliste hinzugefügt.
3. Wählen Sie mindestens eine Prüfoption aus. Vorkonfiguriert sind die Optionen **Boot-Sektoren prüfen**, **Archive prüfen** und **Arbeitspeicher prüfen**. Neben diesen werden auch die Prüfoptionen des manuellen Scanners verwendet.
   - **Boot-Sektoren prüfen**
     - Wenn Sie diese Option wählen, überprüft das Antivirenprogramm den Boot-Sektor der Bereiche, die Sie für die Prüfung vorgesehen haben.
   - **Archive prüfen**
     - Wählen Sie diese Option, wenn Sie archivierte Dateien in den Scan aufnehmen möchten. Zurzeit werden die folgenden Formate unterstützt: ACE, APPLE_SINGLE, ARJ, BZIP2, CAB, GZ, LZH, MAIL, RAR, RAR3, SFXZIP, TAR, ZIP und 7Z.
   - **Arbeitsspeicher prüfen**
     - Wenn Sie den Arbeitsspeicher prüfen, sucht das Antivirenprogramm nach residenten Viren. Sie sollten immer sicherstellen, dass sich im Arbeitsspeicher keine Viren befinden.

Copyright © 1990-2010 Norman ASA

Geplante Überprüfung erstellen

4. Legen Sie Häufigkeit, Zeitpunkt und Datum für die Ausführung der Prüfung fest. Die Voreinträge entsprechen den aktuellen Angaben zu Datum und Uhrzeit (gemäß Ihren Systeminformationen). Sie können auch einen anderen Zeitpunkt wählen.
5. Standardmäßig hat die Aufgabe den Status **Aktiviert**. Um sie zu deaktivieren, entfernen Sie das Häkchen.
6. Klicken Sie auf **Erstellen**.

Alle angesetzten Aufgaben werden als Liste im Dialogfeld **Aufgaben-Editor** angezeigt. Sie können Ihre Aufgabendateien über den Dialog des Aufgaben-Editors anzeigen, bearbeiten, ausführen und löschen. Hier können Sie Aufgaben aktivieren und deaktivieren oder löschen. Mit dem Deaktivieren des Kontrollkästchens **Aktiv** deaktivieren Sie auch die Aufgabe. Um eine Aufgabe zu löschen, setzen Sie das Kontrollkästchen **Löschen** und klicken anschließend auf **Auswahl löschen**.

Der Standardstandort zum Speichern von Ausgabendateien lautet `...Programme\Norman\Tasks`.

Aufgabe entfernen

Um eine Aufgabe zu löschen, wählen Sie mindestens einen Eintrag der Aufgabenliste und klicken auf **Auswahl löschen**.

Ausschlussliste

In der Ausschlussliste enthaltene Dateien werden nicht geprüft. Dateien können beispielsweise vom Prüfvorgang ausgeschlossen werden, wenn sie Fehlalarme auslösen oder die Prüfung zu zeitaufwendig ist. Es wird aber empfohlen, Dateien in der Ausschlussliste in regelmäßigen Abständen durch geplante oder manuelle Scans zu prüfen.

Copyright © 1990-2010 Norman ASA

HINWEIS: Ausschlusslisten sollten äußerst sorgfältig verwaltet werden, da sie ein potenzielles Sicherheitsrisiko darstellen. Das Ausschließen von Dateien oder Bereichen von der Überprüfung geht auf Kosten der Sicherheit.

Ausschlussliste verwenden

Wählen Sie diese Option, um die Ausschlussliste zu aktivieren. Die **Ausschlussliste** dient zum Ausschließen von Dateien, bei denen ein Konflikt mit den Scannern besteht, der sich auf die Leistung des Computers auswirkt.

Dateien von der Überprüfung ausschließen

Legen Sie Dateien, Verzeichnisse oder ganze Laufwerke fest, die nicht auf Malware überprüft werden sollen. Führen Sie die folgenden Schritte durch, um Elemente vom Scanvorgang auszuschließen:

- Klicken Sie auf das Symbol für die Ordnersuche, um nach Dateien und Ordnern zu suchen, oder geben Sie einen Dateinamen, Verzeichnis oder Laufwerksbuchstaben in das Eingabefeld ein.

  Platzhalterzeichen (*/?) werden unterstützt. Setzen Sie den Platzhalter am Anfang oder am Ende des Suchbegriffs. Setzen Sie den Platzhalter nicht in der Mitte des Suchbegriffs.

HINWEIS: Verwenden Sie bei der Angabe auszuschließender Elemente KEINE Anführungszeichen („oder“).

Beispiele

C:\Dir	Schließt alle im angegebenen Verzeichnis und den Unterverzeichnissen enthaltenen Dateien aus.
*.xyz	Schließt alle Dateien mit der Dateierweiterung „.xyz“ aus.
example.exe	Schließt die angegebene Datei ungeachtet des Speicherorts aus.
C:\System\xyz.doc	Schließt diese spezielle Datei aus.

- Bestimmen Sie, welchen Scanner die Ausschlussliste ggf. verwenden sollte.
- Um einen Eintrag der Ausschlussliste hinzuzufügen, klicken Sie auf **Zur Liste hinzufügen**.

HINWEIS: Die Security Suite prüft nicht, ob es die Dateien, Ordner oder Laufwerke, die Sie der Ausschlussliste hinzufügen, tatsächlich gibt. Deshalb dürfen Sie bei der Eingabe von Namen und Pfaden keine Fehler machen.

Netzwerklaufwerke

Sie können auch Netzwerklaufwerke wenn keine Freigaben auf entfernten Computern, auf die Sie Zugriff haben, geprüft werden sollen. Geben Sie ggf. auch den betreffenden Scanner an.

Auswahl löschen

Wenn Sie Einträge aus der Ausschlussliste entfernen möchten, wählen Sie den gewünschten Eintrag und klicken auf **Gewählte entfernen**. Klicken Sie auf **Speichern**, um die Änderungen zu bestätigen.

HINWEIS: Es ist ratsam, die Ausschlussliste in regelmäßigen Abständen zu überarbeiten.

Einstellungen

In diesem Bereich können Sie den automatischen und manuellen Scanner konfigurieren sowie die Funktion „Internet Protection“. Sowohl der automatische als auch der manuelle Scanner verwenden standardmäßig die Norman Sandbox. Nähere Informationen zur Sandbox finden Sie im Abschnitt „Was ist eine Sandbox?“ auf Seite 63. Die Einstellungen des manuellen Scanners sind auch relevant für die Option **Computer prüfen**, den Scanner im Kontextmenü, den Bildschirmschoner-Scanner und den Befehlszeilen-Scanner.

Copyright © 1990-2010 Norman ASA

Automatischer Scanner

Die automatische Prüfung arbeitet im Hintergrund und bietet Ihrem System automatischen Schutz. Sie ist entscheidender Bestandteil der Virenüberwachung und sollte daher immer aktiviert sein.

Automatischen Scanner aktivieren

Durch Auswahl dieser Option starten Sie den automatischen Scanner, durch Aufheben der Auswahl halten Sie ihn an. Es wird empfohlen, den automatischen Scanner immer aktiviert zu lassen.

Wenn der automatische Scanner über die Taskleiste angehalten wird, erscheint in der Taskleiste ein blinkendes gelbes Dreieck. Nähere Informationen finden Sie im Abschnitt „Anwendungssymbol in der Taskleiste“ auf Seite 13. Außerdem werden Sie vom Windows Security Center gewarnt, dass Ihr Computer eventuell gefährdet ist.

1. Achten Sie im Einstellungsmenü des automatischen Scanners darauf, dass die Option **Automatischen Scanner aktivieren** aktiviert ist. Klicken Sie auf **Speichern**, um Ihre Änderungen zu bestätigen.
   - Um die automatische Prüfung zu deaktivieren, entfernen Sie das Häkchen in diesem Kontrollkästchen.
   - Norman Security Suite gibt keine Warnung aus, wenn die automatische Prüfung auf diese Art deaktiviert wird. Das Security Center von Windows warnt Sie jedoch.

HINWEIS: Deaktivieren des Kontrollkästchens Automatischen Scanner aktivieren bedeutet, dass der Scanner so lange deaktiviert wird, bis er manuell wieder eingeschaltet wird.

2. Klicken Sie im Taskleistenmenü auf **Automatischen Scanner starten**.
   - Diese Option wechselt zwischen **Automatischen Scanner starten** und **Automatischen Scanner anhalten**.
   - Falls der Scanner manuell angehalten wurde, wird er beim nächsten Neustart des Computers oder bei der nächsten Installation eines Security Suite-Updates wieder aktiviert.

Copyright © 1990-2010 Norman ASA

Erkannte Viren automatisch entfernen

Der Scanner erkennt und repariert Viren aller Art. Wann immer dies möglich ist, wird eine infizierte Datei repariert und anschließend der Anwendung übergeben. Schlägt die Reparatur fehl, wird der Zugriff auf die infizierte Datei verweigert. Falls eine Datei ausschließlich Malware enthält, wird sie endgültig entfernt.

Benutzermodi

Der Abschnitt zu den Benutzermodi ist in die Module „Lokale Benutzer“ und „Dienste und Remotebenutzer“ eingeteilt. Unter normalen Umständen werden Workstations im Modus **Lokale Benutzer** und Server im Modus **Dienst und Remotebenutzer** ausgeführt. Die Standardeinstellungen bieten ausreichenden Schutz in den meisten Situationen, und wir empfehlen, sie nur dann zu ändern, wenn Ihnen die Folgen in vollem Umfang klar sind.

Lokaler Benutzer

- **Lesen/Ausführen**
  - Hiermit wird der automatische Scanner angewiesen, Dateien zu prüfen, bevor sie geöffnet werden.
  - Beispiel: Wenn ein Benutzer mit Doppelklick eine DOC-Datei auswählt, überprüft der automatische Scanner nicht nur die Datei, sondern auch die entsprechende Anwendung, die geöffnet wird (in diesem Fall MS Word).
- **Beim Lesen und Schreiben prüfen**
  - Hiermit wird der automatische Scanner angewiesen, Dateien zu prüfen, die zur Bearbeitung geöffnet werden und die beispielsweise aus dem Internet heruntergeladen wurden.
  - Bei Auswahl der Prüfoption **Lesen/Ausführen** kann es passieren, dass eine infizierte Datei auf die Festplatte heruntergeladen und gespeichert wird. Allerdings erkennt der automatische Scanner den Virus beim Öffnen der Datei.

Dienste und Remotebenutzer

Dieser Modus greift, wenn Computer mit den Betriebssystemen XP/Vista/Windows 7 abgemeldet werden und theoretisch als Server fungieren können. In diesem Abschnitt wählen Sie aus, ob Dateien geprüft werden sollen, bevor sie verwendet werden und/oder wenn neue Dateien erstellt oder vorhandene Dateien geändert werden. Mit anderen Worten, Sie wählen eine Strategie zur automatischen Prüfung aus, die zum Tragen kommt, wenn Sie aus dem Internet oder von FTP-Servern heruntergeladene Dateien speichern, wenn ein anderer Computer Dateien in eine Netzwerkfreigabe einstellt usw.

- **Schreiben**
  - Hiermit wird der automatische Scanner angewiesen, Dateien zu prüfen, die auf der Festplatte gespeichert wurden, etwa wenn ein Benutzer eine Datei auf einem Server speichert. In diesem Fall prüft der automatische Scanner des betreffenden Servers die Datei.
- **Beim Lesen und Schreiben prüfen**
  - Hierbei handelt es sich um eine Option, die Sie hoffentlich nicht in Anspruch nehmen müssen. Sie kann dann nützlich sein, wenn ein Server infiziert wurde, z. B. weil eine Scanneraktualisierung versäumt wurde. Eine Überprüfung sowohl beim Lesen als auch beim Schreiben sorgt dafür, dass sich der Befall nicht weiter im Netzwerk ausbreitet.

Sandbox verwenden

Die Sandbox-Funktion dient dazu, neue unbekannte Viren zu erkennen. Wählen Sie diese Option, wenn der Scanner auf neue Virusvarianten achten soll. Die Sandbox-Technologie ist speziell darauf abgestimmt, neue E-Mail-, Netzwerk- und Peer-to-Peer-Würmer sowie Dateiviren zu finden und auf unbekannte Gefahren für die Systemsicherheit zu reagieren.

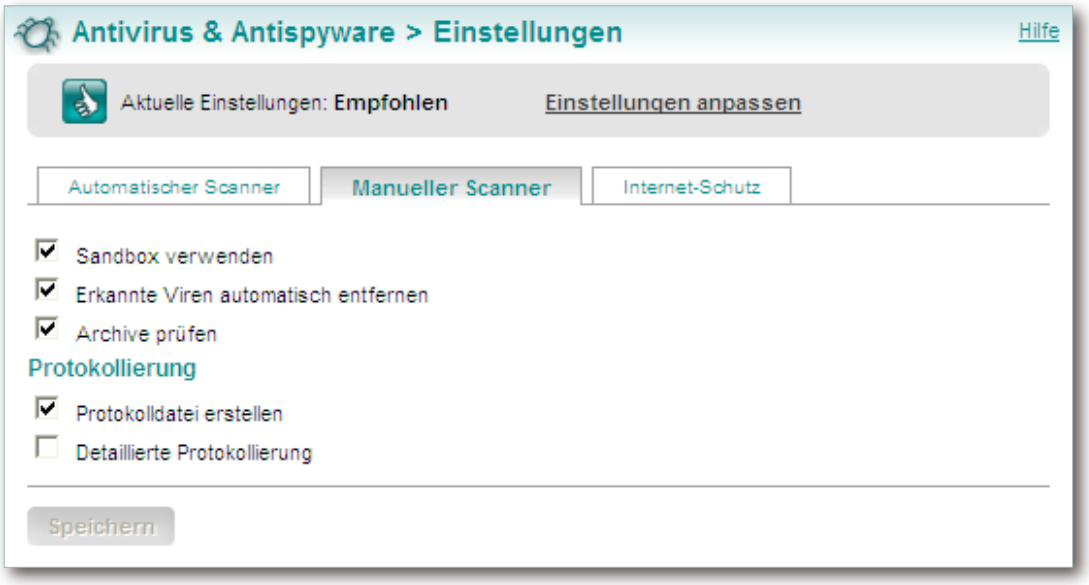
- **Deaktiviert**
  - Die Sandbox-Funktion ist ausgeschaltet.
- **Normal**
  - Dies ist der empfohlene Prüfungsumfang. Wenn diese Option aktiviert ist, prüft die Sandbox alle Schreibvorgänge, und zwar sowohl bei lokalen Benutzern als auch bei Remotebenutzern bzw. -diensten.
- **Erweitert**
  - Diesen Modus können Sie in kritischen Situationen auswählen, z. B. bei einem Virenausbruch im System, für den zunächst keine signaturbasierte Erkennung verfügbar ist. Die Sandbox führt dann sowohl beim Lesen als auch beim Ausführen Überprüfungen durch. Bei Auswahl dieser Option erhöht sich der zeitliche Prüfungsaufwand. Die Leistung wird in der Regel jedoch kaum beeinträchtigt.

Klicken Sie auf **Speichern**, um Ihre Änderungen zu bestätigen.

Copyright © 1990-2010 Norman ASA

Manueller Scanner

Mithilfe des manuellen Scanners können Sie ausgewählte Bereiche Ihres Computers prüfen. Die Überprüfung eines ganzen Laufwerks ist zeitaufwendig. Daher empfiehlt es sich, für die regelmäßige Überprüfung von bestimmten Laufwerken, Ordnern oder Dateien geplante Prüfungen einzurichten. Mithilfe des Aufgaben-Editors können Sie den Bildschirmschoner-Scanner so einrichten, dass manuelle Prüfungen automatisch in Zeiten von Leerlauf oder geringer Computerauslastung erfolgen. Schließlich können Sie den manuellen Scanner auch auf ein Objekt anwenden, indem Sie die entsprechende Option mit der rechten Maustaste auswählen. Die genannten Prüfverfahren verwenden sämtlich die Einstellungen des manuellen Scanners.



Sandbox verwenden

Die Sandbox-Funktion dient dazu, neue unbekannte Viren zu erkennen. Wählen Sie diese Option, wenn der Scanner auf neue Virusvarianten achten soll. Die Sandbox-Technologie ist speziell darauf abgestimmt, neue E-Mail-, Netzwerk- und Peer-to-Peer-Würmer sowie Dateiviren zu finden und auf unbekannte Gefahren für die Systemsicherheit zu reagieren. Bei Auswahl dieser Option erhöht sich der zeitliche Prüfungsaufwand. Die Leistung wird in der Regel jedoch kaum beeinträchtigt.

Erkannte Viren automatisch entfernen

Hierbei versucht die Anwendung, den Virus aus einer infizierten Datei zu entfernen. Wählen Sie diese Option, um infizierte Dateien automatisch zu reparieren. Mit Ausnahme von Bootsektorviren lassen sich die meisten Viren direkt entfernen. Vor dem Entfernen eines Bootsektorvirus wird der Benutzer stets aufgefordert, den Vorgang zu bestätigen. Besteht eine Datei gänzlich aus Malware, wird die gesamte Datei gelöscht.

Archive prüfen

Wählen Sie diese Option, wenn Sie archivierte Dateien in den Scan aufnehmen möchten. Zurzeit werden die folgenden Formate unterstützt: ACE, APPLE_SINGLE, ARJ, BZIP2, CAB, GZ, LZH, MAIL, RAR, RAR3, SFXZIP, TAR, ZIP und 7Z.

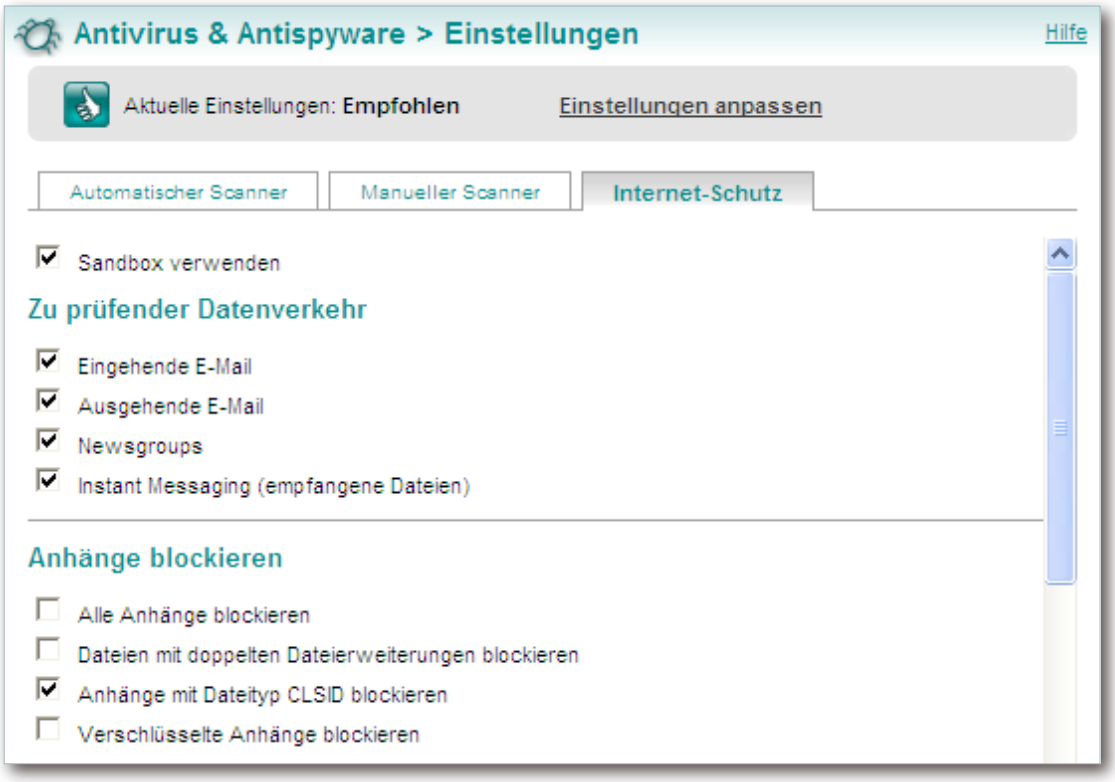
Protokollierung

- **Protokolldatei erstellen**
  Hiermit wird bei jedem Ausführen eines manuellen Scans eine Protokolldatei im Ordner „C:\Programme\Norman\Logs“ erstellt. Wenn Sie diese Option deaktivieren, werden für manuelle Prüfungen keine Protokolldateien erstellt. Standardmäßig ist diese Option aktiviert.
- **Detaillierte Protokollierung**
  Bei der ausführlichen Protokollierung wird ein Bericht mit vielen Einzelheiten erstellt, in dem jede durchsuchte Datei, Prüfdauer pro Datei, Status usw. angegeben ist.

Copyright © 1990-2010 Norman ASA

Internet Protection

Dieser Filter schützt vor Viren, die sich über Internet-Mail und Newsreader verbreiten. Die meisten Viren, die heutzutage erfasst werden, verbreiten sich über E-Mail-Nachrichten. Dieses Filtermodul ist gedacht, ein- und ausgehende Mails und News abzufangen und alle infizierten Anlagen von unerwünschten Inhalten zu bereinigen bzw. sie zu blockieren. Es kann je nach Inhalt und Dateierweiterung sowohl E-Mails auf bekannte Viren prüfen als auch Dateianhänge blockieren.



Sandbox verwenden

Die Sandbox-Funktion dient dazu, neue unbekannte Viren zu erkennen. Wählen Sie diese Option, wenn der Scanner auf neue Virusvarianten achten soll. Die Sandbox-Technologie ist speziell darauf abgestimmt, neue E-Mail-, Netzwerk- und Peer-to-Peer-Würmer sowie Dateiviren zu finden und auf unbekannte Gefahren für die Systemsicherheit zu reagieren. Bei Auswahl dieser Option erhöht sich der zeitliche Prüfungsaufwand. Die Leistung wird in der Regel jedoch kaum beeinträchtigt. Weitere Informationen zur Sandbox-Technologie finden Sie in „Anhang A“ auf Seite 63.

Copyright © 1990-2010 Norman ASA

Zu prüfender Datenverkehr

Wählen Sie aus, welche Elemente des Internet-Verkehrs gescannt werden sollen. Standardmäßig werden alle gescannt.

- **Eingehende Mail (POP3),**
  - Scannt alle E-Mails, die Sie von anderen empfangen. Wie bereits erwähnt, selbst Ihr bester Freund oder Geschäftspartner kann Ihnen in Unkenntnis einen Virus senden.
- **Ausgehende Mail (SMTP),**
  - Scannt alle E-Mails, die von Ihrem System gesendet werden. Wenn Ihr Computer durch Malware infiziert ist und Sie sich dessen nicht bewusst sind, könnte es passieren, dass Sie unbeabsichtigt infizierte E-Mails z. B. an Freunde und Geschäftspartner senden.
- **Newsgroups (NNTP),**
  - Prüft den Verkehr zwischen Ihrem Computer und anderen Teilnehmern in der Gruppe/dem Forum, in der/dem Sie sich gerade befinden.
- **Instant Messaging (empfangene Dateien),**
  - Prüft den Dateitransfer während Instant-Messaging-Sitzungen mit MSN Messenger und Windows Messenger. Wenn diese Option ausgewählt wird, werden eingehende Dateien auf Malware geprüft. Wenn eine Datei infiziert ist, werden Sie mit einer Popup-Meldung von dem Vorfall in Kenntnis gesetzt.
  - Es werden nur Dateitransfers geprüft. Infizierte Links stellen also weiterhin eine Gefahr dar.

Beachten Sie, dass transferierte Dateien in dem Moment geprüft werden, in dem sie in das Verzeichnis ...\Temporäre Internetdateien **geschrieben werden. Wenn Malware entdeckt wird, handelt es sich wahrscheinlich um eine TMP-Datei, die unter Quarantäne gestellt wird. Zur Wiederherstellung einer in Quarantäne befindlichen TMP-Datei markieren Sie die gewünschte Datei, und speichern Sie diese dann mithilfe der Option** Speichern unter **aus dem Kontextmenü (Rechtsklick) unter ihrem ursprünglichen Namen und mit der ursprünglichen Erweiterung. Nähere Informationen finden Sie im Abschnitt „Quarantäne“ auf Seite 18.**

Anhänge blockieren

Diese Funktion ist besonders hilfreich, wenn E-Mail-Würmer im Umlauf sind und der Wurm anhand seines Namens identifiziert werden kann. Das Sperren von Anhängen eignet sich auch dazu, den Empfang bestimmter Dateitypen in Ihrer Mailbox zu verhindern. Gesperrte Anhänge werden nicht gelöscht, sondern in den Quarantänebereich verschoben. Sie können Anhänge auch anhand des Namens oder der Erweiterung sperren, indem Sie die entsprechenden Informationen eingeben. Nachstehend werden die verfügbaren Konfigurationsoptionen kurz erläutert:

- **Alle Anhänge blockieren**
  - Alle Anhänge werden gesperrt.
- **Dateien mit doppelten Dateierweiterungen blockieren**
  - Viele Würmer und E-Mail-Viren fügen Dateien eine zusätzliche Erweiterung hinzu, z. B. **Dateiname.jpg.vbs**. Die meisten E-Mail-Clients verbergen die letzte Erweiterung, sodass die Anlage scheinbar nur die Erweiterung JPG hat. Dieses Verfahren wird jedoch nicht nur von Viren verwendet – zulässige Dateien mit Namen wie **Meinedatei.hlp.zip** und **Aufgabenliste_20.dez.doc** werden ebenfalls als Doppelerweiterungen behandelt.
- **Anhänge mit Dateityp CLSID blockieren**
  - Einige neuere Würmer und E-Mail-Viren wenden ein CLSID-Verfahren an, um E-Mail-Scanner und Schutzsoftware zu täuschen. Dabei machen sie sich zunutze, dass es unter Windows möglich ist, eine EXE-Erweiterung durch eine {...}-Erweiterung zu ersetzen und so die Sperrung von EXE-Dateien zu umgehen. Da es bei einwandfreien Anlagen keinen Grund gibt, diese Erweiterung zu verwenden, wird dieses Verhalten standardmäßig blockiert.
- **Verschlüsselte Anhänge blockieren**
  - Je nach verwendeten Tools sind komprimierte und verschlüsselte Dateien in der Regel schwerer auf Viren zu überprüfen als einfache Dateianhänge. Deshalb bietet das Antivirenprogramm die Möglichkeit, solche Anhänge komplett zu blockieren.

Copyright © 1990-2010 Norman ASA

Anhangliste

Mit dieser Funktion wählen Sie explizit Anhänge aus, die Sie sperren – oder zertifizieren – möchten. Sie können den genauen Namen eines Anhangs eingeben oder das Platzhalterzeichen (*) verwenden, um bestimmte Erweiterungen zu sperren. Der Eintrag wird im Listenfeld angezeigt. Sie können ihn zu einem späteren Zeitpunkt bearbeiten oder entfernen.

Beispielsweise würden Sie `*.exe` eingeben, um alle Anhänge mit der EXE-Erweiterung zu sperren oder zuzulassen. Setzen Sie den Platzhalter am Anfang oder am Ende des Suchbegriffs. Setzen Sie den Platzhalter nicht in der Mitte des Suchbegriffs.

- **Alle aufgeführten Anhänge blockieren**
  - Alle Namen, die Sie mit **Hinzufügen** in die Liste aufnehmen, werden **gesperrt**.
  - Klicken Sie auf **Speichern**, um Ihre Änderungen zu bestätigen.
- **Alle Anhänge außer den aufgeführten blockieren**
  - Alle Namen, die Sie mit **Hinzufügen** in die Liste aufnehmen, werden **gesperrt**.
  - Klicken Sie auf **Speichern**, um Ihre Änderungen zu bestätigen.

HINWEIS: Es ist sehr wichtig, dass Sie sorgfältig zwischen diesen beiden Optionen unterscheiden, da sie zwei Extreme darstellen: die gesamte Liste SPERREN oder die gesamte Liste ZULASSEN.

Nähere Informationen zum Thema finden Sie in der Hilfedatei der Anwendung.

Einträge entfernen

Markieren Sie mindestens einen Eintrag, und klicken Sie auf **Gewählte entfernen**. Klicken Sie auf **Speichern**, um Ihre Änderungen zu bestätigen.

Ports

Unter den zahlreichen Protokollen für die Kommunikation zwischen Computern gibt es einige, die für die Internetnutzung unerlässlich sind. Aus Gründen der Normierung sind in den Protokollen bereits Portnummern zugewiesen.

Portnummern

Manche der Protokolle für die Kommunikation zwischen Computern sind wichtig für die Internetnutzung. Aus Gründen der Normierung sind in den Protokollen bereits Portnummern zugewiesen. Im Bereich „Zu prüfender Datenverkehr“ wählen Sie aus, welcher Internetverkehr geprüft werden soll. Dieses Dialogfeld identifiziert z. B. die für das Senden und Empfangen von E-Mails benötigten Protokolle und die zugehörige, dem Industriestandard entsprechende Portnummer auf dem Computer.

Möglicherweise haben Sie einem oder mehreren der unterstützten, hier aufgelisteten Protokolle verschiedene Portnummern zugewiesen. In diesem Fall müssen Sie die aktuelle Portnummer für das/die betroffene(n) Protokoll(e) eingeben.

Derzeit werden die unten aufgeführten Protokolle unterstützt. Die Liste wird nach Bedarf aktualisiert. Die Portnummern und Funktionen sind bereits im Dialogfeld festgelegt:

- **Eingehende E-Mail (POP3)**
  Die Abkürzung POP (Port 110) steht für „Post Office Protocol“.
- **Ausgehende E-Mail (SMTP)**
  Die Abkürzung SMTP (Port 25) steht für „Simple Mail Transport Protocol“.
- **Newsgroups (NNTP)**
  Die Abkürzung NNTP (Port 119) steht für „Network News Transfer Protocol“.

Copyright © 1990-2010 Norman ASA

Weitere Prüfverfahren

Bildschirmschoner-Scanner aktivieren

Wenn Sie den Bildschirmschoner-Scanner aktivieren, wird Ihr System bei Leerlauf auf Viren geprüft. Die Dauer der Nichtbenutzung ist als der Zeitraum definiert, in dem das System keine Aktivitäten verzeichnet, d. h. Eingaben weder über die Tastatur noch über die Maus erfolgen.

Beim Start des Bildschirmschoners startet der manuelle Scanner eine Prüfung aller Festplatten. Sobald der Computer etwa durch eine Mausbewegung oder Tasteneingabe wieder in Betrieb genommen wird, hält die Bildschirmschoner-Prüfung an. Falls die Prüfung zu diesem Zeitpunkt noch nicht abgeschlossen sein sollte, wird sie bei der nächsten Leerlaufphase an dem Punkt, wo sie unterbrochen wurde, fortgesetzt.

1. Gehen Sie auf **Antivirus & Antispyware**, und wählen Sie die Option **Bildschirmschoner-Scanner aktivieren**.
   - Das Dialogfeld „Eigenschaften anzeigen“ der Windows-Systemsteuerung wird angezeigt.

2. Wählen Sie aus der Dropdown-Liste **Bildschirmschoner** die Option **Norman-Screensaver**.
   - Um einen Probelauf des Bildschirmschoners zu sehen, klicken Sie auf **Vorschau**.
   - Die Vorschau beenden Sie durch Betätigen einer beliebigen Taste oder durch Bewegen der Maus.
3. Klicken Sie auf **OK**, um Ihre Änderungen zu bestätigen.

Sobald der Norman-Screensaver durch die nächste Leerlaufphase aktiviert wird, beginnt der manuelle Scanner mit der Prüfung der Festplatten, wobei der Prüfungsfortschritt ständig angezeigt wird. Den Bildschirmschoner-Scanner beenden Sie durch Betätigen einer beliebigen Taste oder durch Bewegen der Maus.

HINWEIS: Die Bildschirmschoner-Prüfung verwendet die gleichen Einstellungen wie die des manuellen Scanners.

Kontextmenü-Scanner

Hierbei handelt es sich um einen manuellen Scanner, mit dem Sie aktuell markierte Dateien oder Ordner prüfen lassen können, indem Sie mit der rechten Maustaste das Windows-Kontextmenü aufrufen.

- Klicken Sie dazu mit der rechten Maustaste auf eine Datei oder einen Ordner.
  - Dies funktioniert beispielsweise im Windows Explorer oder auf dem Desktop.
- Wählen Sie aus dem Popup-Menü die Option **Prüfung auf Viren**.
- Das Dialogfeld **Manueller Scanner** wird angezeigt. Sie können den Computer nach weiteren Dateien oder Ordnern **Durchsuchen**, die geprüft werden sollen, und den Prüfvorgang mithilfe der Optionen **Start**, **Pause** oder **Stop** entsprechend steuern.

Befehlszeilen-Scanner

Sie können statt des Scanners mit Benutzeroberfläche auch die Befehlszeilenprüfung einsetzen, etwa um Stapelaufträge und andere Prüfaufgaben über die Befehlszeile auszuführen. Die Befehlszeilenprüfung ist eine gute Alternative für Benutzer, die mit dieser Umgebung vertraut sind.

Copyright © 1990-2010 Norman ASA

Der Befehlszeilen-Scanner hat dieselben Basisfunktionen wie die menügesteuerten Scanner und hängt nicht von anderen Modulen ab. Er kann auch über Stapeldateien ausgeführt werden.

Starten des Befehlszeilen-Scanners

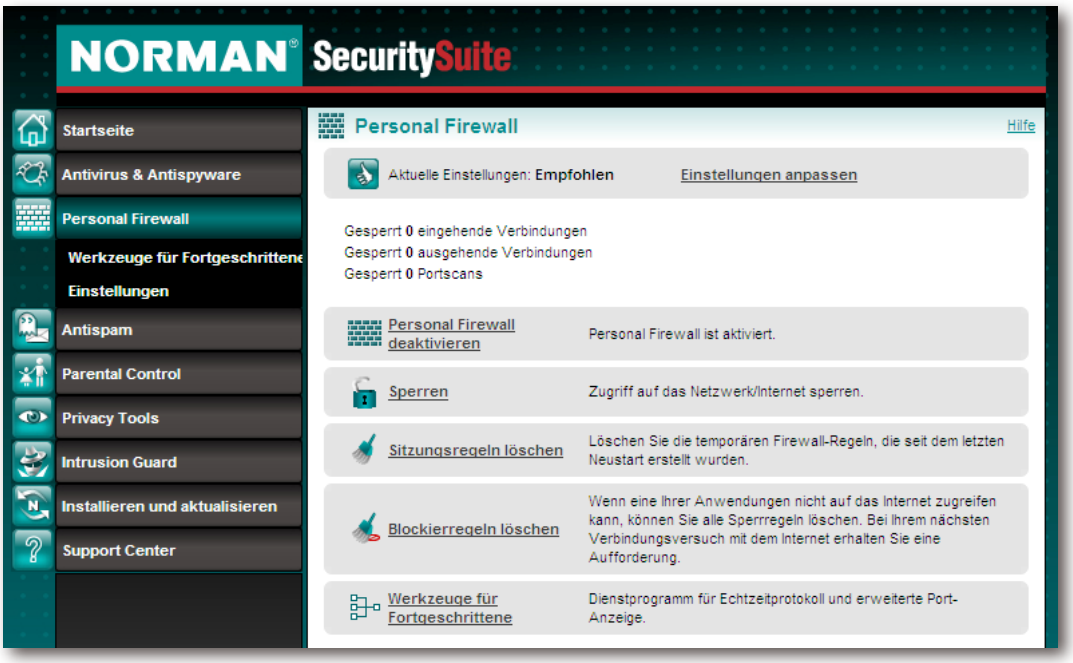
1. Rufen Sie die Eingabeaufforderung auf.
   - Wählen Sie **Start** > **Ausführen**.
   - Geben Sie „CMD“ ein, und klicken Sie auf **OK**, oder drücken Sie die **Eingabetaste**.
2. Gehen Sie in das Verzeichnis, in der die Anwendung „Antivirus & Antispyware“ zu finden ist.
   - Der Standardpfad lautet `C:\Programme\Norman\nvc\bin\`.
3. Geben Sie die gewünschten Parameter ein, und drücken Sie die Eingabetaste.
   - Um eine Liste der verfügbaren Parameter aufzurufen, geben Sie folgenden Befehl ein:
     ```
     nvcc /?
     ```
   - Die Syntax hierfür lautet:
     ```
     nvcc [Laufwerk]:[Pfad] [/Parameter] [Eingabetaste]
     ```
   - Vor jedem Parameter, den Sie verwenden, muss ein Leerzeichen stehen.

Copyright © 1990-2010 Norman ASA

Personal Firewall

Stellen Sie den Installationsassistenten fertig (nähere Informationen dazu im Abschnitt „Installationsassistent“ auf Seite 12). Öffnen Sie die Anwendung „Security Suite“, und wählen Sie im linken Menü die Option **Personal Firewall**. Nähere Informationen zum Öffnen der Anwendung finden Sie im Abschnitt „Erste Schritte“ auf Seite 13, Informationen zu ihrem Zweck und ihrer Funktionsweise im Abschnitt „Personal Firewall“ auf Seite 6. Informationen zum Initialisieren der Personal Firewall finden Sie im Abschnitt „Installationsassistent“ auf Seite 12.

Hauptseite



Dieses Kapitel behandelt die Konfiguration der Firewall-Anwendung, das Erstellen der Regeln für ein- und ausgehende Anwendungen, das Anzeigen des Datenverkehrs und weitere Themen. Die Anwendung unterscheidet zwischen erfahrenen und unerfahrenen Benutzern. Während der unerfahrene Benutzer vom Installationsassistenten geführt wird, haben erfahrene Benutzer die Möglichkeit, die erweiterten Einstellungen bis ins Detail zu konfigurieren.

Einstellungen anpassen

Klicken Sie auf diese Option, um die Standardwerte zu bearbeiten. Nähere Informationen finden Sie im Abschnitt „Einstellungen“ für die Personal Firewall auf der Seite 39. Allgemeine Informationen zur Wahl zwischen empfohlenen und benutzerdefinierten Einstellungen finden Sie im Abschnitt „Einstellungen der Security Suite“ auf Seite 15.

Statistik

Die Statistik zeigt Informationen zu blockierten ein- und ausgehenden Verbindungen und Portscans an.

- **Anzahl blockierter eingehender Verbindungen**.
  Es wurde versucht, auf Ihren Computer zuzugreifen, und der Versuch wurde blockiert, möglicherweise weil Sie nicht die erforderliche Software installiert haben. Solche Verbindungen sind selten bösartig. Meist handelt es sich um zulässige Serveranfragen.
- **Anzahl blockierter ausgehender Verbindungen**.
  Die Anzahl der ausgehenden Verbindung, die von mindestens einer Regel blockiert wurden. Falls eine große Anzahl ausgehender Verbindungen gesperrt sind, sollten Sie die entsprechenden Regeln überprüfen.
- **Anzahl blockierter Portscans**.
  Zeigt an, wie viele systematische Versuche erfolgt sind, nach offenen Ports zu suchen. Manchmal suchen Viren nach offenen Ports, um sich zu verbreiten, allerdings könnte es sich auch um einen zulässigen Vorgang seitens der Verwaltungssoftware handeln.

Copyright © 1990-2010 Norman ASA

Personal Firewall deaktivieren (aktivieren)

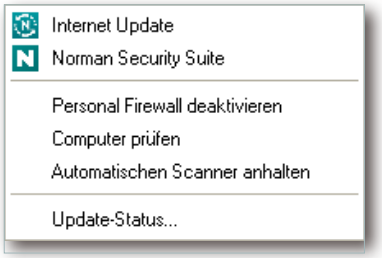
Durch Anklicken des Links wechseln Sie zwischen aktiviertem und deaktiviertem Status der Personal Firewall. Sie können die Personal Firewall wahlweise auf der Hauptseite der Anwendung oder über das Taskleistenmenü starten.

- Gehen Sie auf die Hauptseite der Personal Firewall, und wählen Sie die Option **Personal Firewall deaktivieren**.

HINWEIS: Das Windows Security Center gibt bei Deaktivierung der Firewall eine Warnmeldung aus.

oder

- Klicken Sie mit der rechten Maustaste auf das Symbol in der Taskleiste, und wählen Sie **Personal Firewall deaktivieren**.



HINWEIS: Diese Option ist unter Windows Vista nicht verfügbar. Dort müssen Sie die Personal Firewall über die Konsole aktivieren bzw. deaktivieren.

Sperren

Durch Anklicken des Links wechseln Sie zwischen Sperren und Entsperren aller Netzwerkzugänge einschließlich derjenigen zum Internet. Diese Funktion könnten Sie nutzen, wenn Ihr Computer in Ihrer Abwesenheit weiterläuft.

Sitzungsregeln löschen

Wählen Sie diese Option, um die temporären Firewall-Regeln zu löschen, die seit dem letzten Neustart des Computers erstellt wurden. Temporäre Firewall-Regeln werden im Verlauf einer Arbeitssitzung, also zwischen zwei Neustarts, erstellt, wenn Sie im Popup-Dialogfeld der Firewall die Option **für diese Sitzung** auswählen. Dieses Dialogfeld erscheint, wenn ein Vorgang eine Entscheidung Ihrerseits erfordert, ob der Vorgang zugelassen oder verweigert werden soll. Unter einem Vorgang ist beispielsweise der Versuch eines Programms zu verstehen, auf das Internet zuzugreifen. Sie werden aufgefordert, das Aussetzen der Regeln zu bestätigen.

Blockierregeln löschen

Wenn Sie keinen Zugriff auf das Internet bzw. Netzwerk haben, kann es sein, dass eine Regel möglicherweise die Verbindung blockiert. Klicken Sie auf diese Option, um alle Blockierregeln zu entfernen. Bei Ihrem nächsten Zugriffsversuch auf das Internet werden Sie aufgefordert, dies zu bestätigen.

Werkzeuge für Fortgeschrittene

Siehe den nächsten Abschnitt.

Copyright © 1990-2010 Norman ASA

Werkzeuge für Fortgeschrittene

Die Werkzeuge für Fortgeschrittene umfassen den Regelassistenten, das Echtzeitprotokoll-Dienstprogramm, die Erweiterte Port-Anzeige sowie die Funktion zum Importieren und Exportieren von Personal Firewall-Regeln. Mit diesen Werkzeugen können Sie erweiterte Aspekte dieser Anwendung verwalten.

Die Werkzeuge für Fortgeschrittene sind für professionelle Benutzer gedacht. Ausnahme ist der Regelassistent, der für unerfahrene Benutzer ideal ist. Sie können im Dialogfeld des Regelassistenten zwischen Assistentenmodus und erweitertem Modus wechseln.

Sie können die Regeln mithilfe des Regelassistenten festlegen oder bearbeiten. Die Firewall-Regeln sind notwendig, um vertrauenswürdigen Anwendungen den Internetzugang zu ermöglichen und nicht vertrauenswürdige Verbindungen zu blockieren. Die Firewall nutzt ausgefeilte Tarntechniken, um Ihren Computer gegenüber dem Internet abzuschirmen und zu verbergen. Sie können die Computeraktivitäten mithilfe des Echtzeitprotokoll-Dienstprogramms und der erweiterten Port-Anzeige überwachen.

Personal Firewall > Werkzeuge für Fortgeschrittene
Hilfe
Regelassistent
Dauerhafte Regeln anzeigen und ändern.
Dienstprogramm für Echtzeitprotokoll-
Aktivität mit Netzwerkbezug, Konfigurationsdetails.
Erweiterte Port-Anzeige
Zeigen Sie den Port-Status an, und bearbeiten Sie die entsprechenden Regeln.
Personal Firewall-Regeln exportieren
Sicherheitskopie für Personal Firewall-Regeln und -Einstellungen anlegen.
Personal Firewall-Regeln importieren
Sicherheitskopie der Personal Firewall-Regeln und -Einstellungen wiederherstellen. Vorhandene Regeln werden überschrieben.

Regelassistent

Regeln werden benötigt, um „vertrauenswürdigen“ Anwendungen den Zugriff auf das Internet zu ermöglichen. Darauf sind viele moderne Programme angewiesen. Die Firewall hat Regeln für vertrauenswürdige Programme auf Ihrem Computer installiert, als Sie den Installationsassistenten ausgeführt haben. Es können jedoch auch Programme installiert sein, die von der Firewall nicht erkannt werden oder erst nach der Installation der Firewall hinzugekommen sind. Wenn ein solches Programm versucht, eine Verbindung zum Internet herzustellen, öffnet die Personal Firewall ein Popup-Fenster, in dem Sie über diesen Vorgang informiert werden und entscheiden können, ob der Zugriff zugelassen oder verweigert werden soll.

NORMAN SecuritySuite
Hosts-Datei wurde geändert
Ihre Hosts-Datei wurde geändert. Diese Datei konvertiert Namen wie www.norman.com in IP-Adressen und kann von bösartigen Anwendungen dazu missbraucht werden, Ihren Computer an eine falsche Adresse weiterzuleiten. Haben Sie die Datei absichtlich geändert?
Verweigern
Zulassen
Änderungen anzeigen

Copyright © 1990-2010 Norman ASA

Regeln für eingehende Verbindungen können Sie mit der Personal Firewall nicht erstellen. Diese werden auf der Basis der Entscheidungen im Servermodus der Personal Firewall angelegt. Dies erfolgt dynamisch und automatisch sowie auf Grundlage von Serverrechten. Dabei handelt es sich um einen intelligenten Mechanismus der Firewall, der Zugriffsversuche von außen auf eine Gruppe von Ports auswertet. Legitimen Anforderungen wird der Zugriff für die relevanten Ports gewährt. Wenn dies nicht mehr erforderlich ist, werden die Ports automatisch geschlossen.

Wenn Sie den Installationsassistenten für die Personal Firewall ausführen, können Sie entweder als unerfahrener oder erfahrener Benutzer vorgehen. Der Regelassistent unterscheidet je nach gewähltem Benutzerniveau.

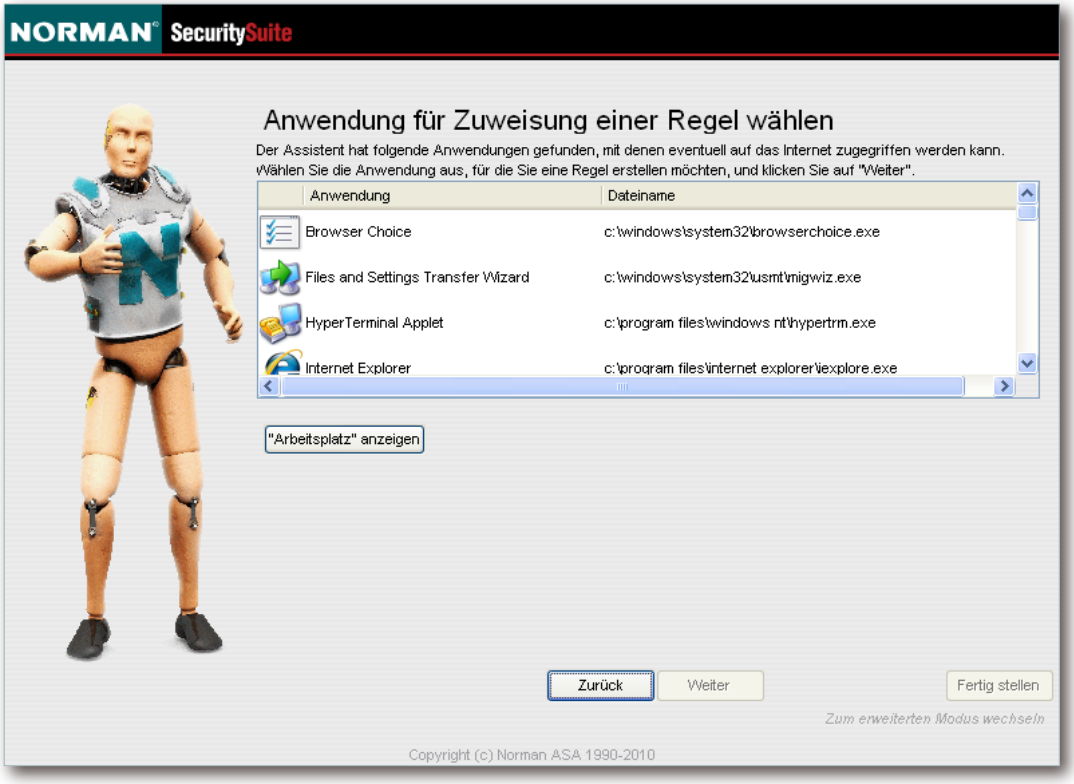
TIPP

BENUTZERMODUS WECHSELN: In der rechten unteren Ecke des Regelassistenten-Dialogfelds finden Sie die Option, den Benutzermodus zu bestimmen. Die Option wechselt zwischen *Zum assistierten Modus wechseln* **und** *Zum erweiterten Modus wechseln*.

Unerfahrenes Niveau (assistierter Modus)

Gehen Sie nacheinander auf **Personal Firewall > Werkzeuge für Fortgeschrittene**, und klicken Sie auf **Regelassistent**, um das Regelassistent-Dialogfeld zu öffnen.

1. **Regelassistent**
   - Wählen Sie **Ich möchte eine neue Regel erstellen**. Klicken Sie dann auf **Weiter**.



2. **Anwendung für Zuweisung einer Regel wählen.**
   - Daraufhin wird eine Liste mit infrage kommenden Anwendungen angezeigt. Markieren Sie die Anwendung Ihrer Wahl, indem sie diese anklicken. Wählen Sie **Arbeitsplatz anzeigen**, um Ihren Computer nach Programmenzu durchsuchen, die nicht in der Liste aufgeführt sind. Klicken Sie auf **Weiter**, um fortzufahren.
3. **Aktion für diese Anwendung?**
   - Wählen Sie **Zulassen** oder **Verweigern**, um den Internetzugriff der Anwendung zuzulassen oder zu verweigern. Klicken Sie auf **Weiter**, um fortzufahren.

Copyright © 1990-2010 Norman ASA

4. **Ist dies eine Serveranwendung?**
   - Finden Sie heraus, ob es sich um eine Serveranwendung handelt. Serveranwendungen halten Ports sichtbar offen – sodass sich der Computer wie ein Server verhält – und ermöglichen anderen Computern so den Zugriff. Falls Sie sich nicht sicher sind, wählen Sie **Nein**. Klicken Sie auf **Weiter**, um fortzufahren.

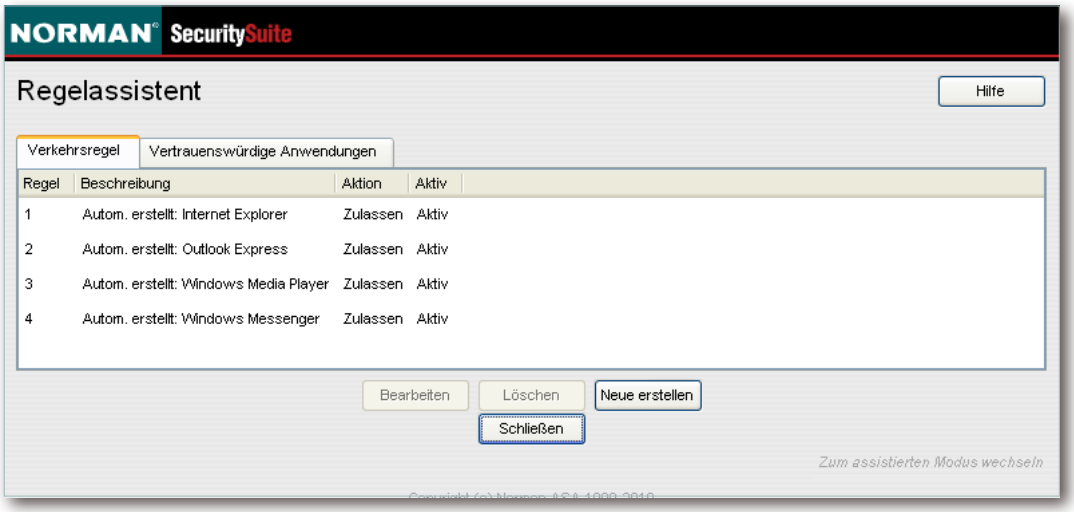
TIPP

Sie werden später von der Firewall zur Bestätigung aufgefordert, wenn die Anwendung Serverrechte anfordert. Regeln lassen sich stets auch später noch ändern.

5. **Zusammenfassung**
   - Ein Dialogfeld mit einer Zusammenfassung wird angezeigt. Klicken Sie auf **Fertig stellen**, um die neue Regel zu erstellen.
   - Die Regel tritt in Kraft, sobald sie erstellt wurde.

Erfahrenes Niveau (erweiterter Modus)

Gehen Sie nacheinander auf **Personal Firewall > Werkzeuge für Fortgeschrittene**, und klicken Sie dann auf **Regelassistent**. Daraufhin wird ein Dialogfeld angezeigt, in dem vorhandene Regeln und ihr Status aufgelistet sind.



1. Klicken Sie auf **Neue erstellen**, und füllen Sie die erforderlichen Felder aus.
2. Klicken Sie zum Bestätigen auf **OK**.

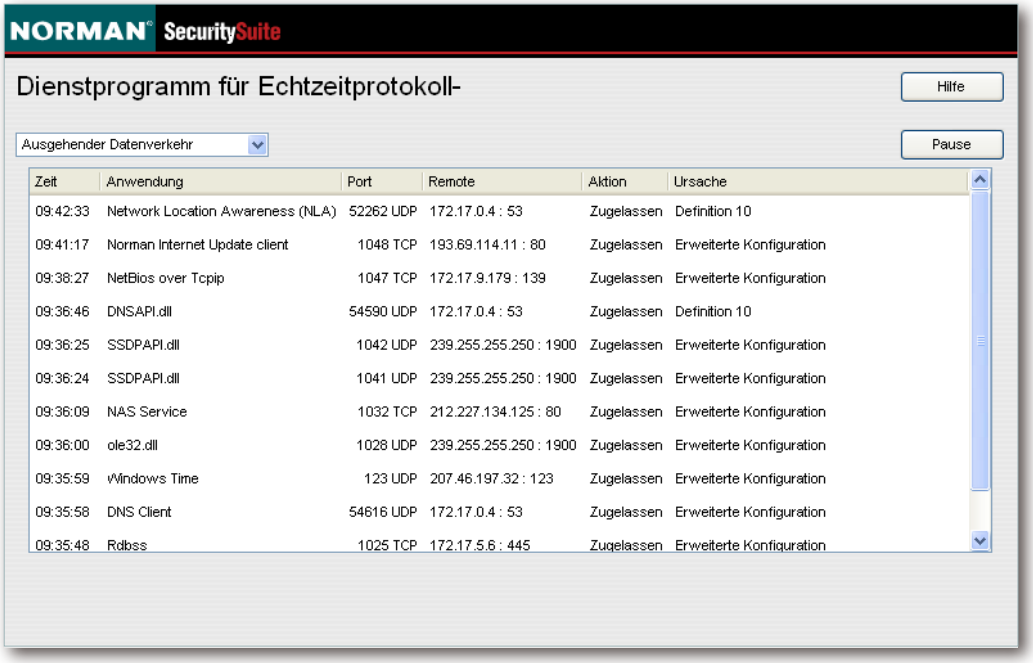
Eine ausführliche Beschreibung aller Felder finden Sie in den Hilfedateien der Anwendung.

Copyright © 1990-2010 Norman ASA

Dienstprogramm für Echtzeitprotokoll

Die Personal Firewall nutzt ausgefeilte Tarntechniken, um Ihren Computer gegenüber dem Internet abzuschirmen und zu verbergen. Mit zwei weiteren Funktionen können Sie die Aktivitäten auf Ihrem Computer überwachen: **Dienstprogramm für Echtzeitprotokoll** und **Erweiterte Port-Anzeige**.

Gehen Sie nacheinander auf **Personal Firewall > Werkzeuge für Fortgeschrittene**, und klicken Sie dann auf **Dienstprogramm für Echtzeitprotokoll**. Klicken Sie mit der rechten Maustaste auf einen Eintrag, um Details anzuzeigen und ggf. die Konfiguration für die betreffende Anwendung zu ändern.


NORMAN SecuritySuite
Dienstprogramm für Echtzeitprotokoll-
Hilfe
Ausgehender Datenverkehr
Pause
Zeit Anwendung Port Remote Aktion Ursache
09:42:33 Network Location Awareness (NLA) 52262 UDP 172.17.0.4 : 53 Zugelassen Definition 10
09:41:17 Norman Internet Update client 1048 TCP 193.69.114.11 : 80 Zugelassen Erweiterte Konfiguration
09:38:27 NetBios over Tcpip 1047 TCP 172.17.9.179 : 139 Zugelassen Erweiterte Konfiguration
09:36:46 DNSAPI.dll 54590 UDP 172.17.0.4 : 53 Zugelassen Definition 10
09:36:25 SSDPAPI.dll 1042 UDP 239.255.255.250 : 1900 Zugelassen Erweiterte Konfiguration
09:36:24 SSDPAPI.dll 1041 UDP 239.255.255.250 : 1900 Zugelassen Erweiterte Konfiguration
09:36:09 NAS Service 1032 TCP 212.227.134.125 : 80 Zugelassen Erweiterte Konfiguration
09:36:00 ole32.dll 1028 UDP 239.255.255.250 : 1900 Zugelassen Erweiterte Konfiguration
09:35:59 Windows Time 123 UDP 207.46.197.32 : 123 Zugelassen Erweiterte Konfiguration
09:35:58 DNS Client 54616 UDP 172.17.0.4 : 53 Zugelassen Erweiterte Konfiguration
09:35:48 Rdbss 1025 TCP 172.17.5.6 : 445 Zugelassen Erweiterte Konfiguration

Ausgehender Datenverkehr

Das Protokoll hält Folgendes fest: zu welcher **Zeit** eine **Anwendung** auf das Internet zugegriffen hat, den Programmnamen und den benutzten **Port**. Ferner vermerkt es die IP-Adresse, den Port des **Remote-Computers** und die jeweilige **Aktion**. Die **Aktion** wird entweder zugelassen oder verweigert. Die **Ursache** ist entweder, dass eine permanente Regel oder eine Sitzungsregel für die betreffende Aktion bzw. Anwendung vorliegt, sofern sie in der **Erweiterten Konfiguration** definiert ist, oder eine Zeitüberschreitung bei der Benutzeraufforderung.

Anforderungen von Serverrechten

Das Protokoll hält Folgendes fest: zu welcher **Zeit** eine **Anwendung** auf den Computer vom Internet aus zugegriffen hat und den benutzten **Port**. Ferner vermerkt es die IP-Adresse, den Port des **Remote-Computers** und die jeweils von der Personal Firewall ergriffene **Aktion**. Die **Aktion** wird entweder zugelassen oder verweigert. Die **Ursache** ist entweder, dass eine permanente Regel oder eine Sitzungsregel für die betreffende Aktion bzw. Anwendung vorliegt, die in der **Erweiterten Konfiguration** definiert ist, oder dass keine empfangende Anwendung vorhanden ist. Der häufigste Grund für die Ablehnung von Anforderungen von Serverrechten ist, dass Ihr Computer nicht über die erforderliche Software zur Interpretation der Anfrage verfügt. Mit anderen Worten, es liegen keine Serverrechte vor, die der Anforderung entsprechen.

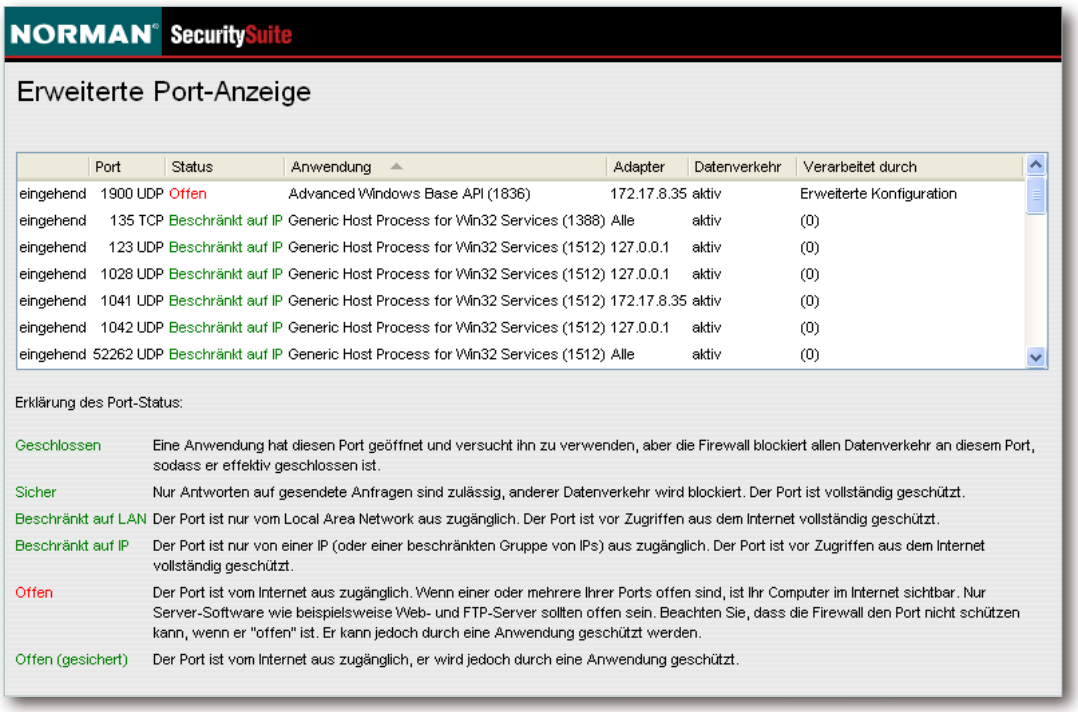
Um Daten von einem anderen Computer im Netzwerk zu empfangen, öffnet eine Anwendung mindestens einen empfangsbereiten Port. Hierbei ist zu beachten, dass Anforderungen von Serverrechten keine eingerichteten Verbindungen darstellen, sondern nur Anforderungen von Verbindungen. Allerdings öffnet eine Anwendung manchmal auch einen empfangsbereiten Port, um die Antwort eines Computer zu empfangen, an den sie Daten versendet hat. Die Personal Firewall lässt solche Antworten automatisch zu. Ein Mechanismus der Personal Firewall ermittelt, ob eine Anwendung einen Port absichtlich geöffnet hat oder ob die Anwendung eine unerwünschte Anfrage erhält, als handele es sich um einen Server. Daraufhin fordert die Personal Firewall den Benutzer auf zu bestätigen, dass die Anwendung Serverrechte erhalten soll.

Copyright © 1990-2010 Norman ASA

Erweiterte Port-Anzeige

Die erweiterte Port-Anzeige bietet eine Übersicht aller Aktivitäten an den Ports des aktuellen Computers. Dieses Dienstprogramm dient zur manuellen Prüfung, ob Ihr Computer von Malware befallen ist.

Gehen Sie nacheinander auf **Personal Firewall > Werkzeuge für Fortgeschrittene > Erweiterte Port-Anzeige**.


NORMAN SecuritySuite
Erweiterte Port-Anzeige
Port Status Anwendung Adapter Datenverkehr Verarbeitet durch
eingehend 1900 UDP Offen Advanced Windows Base API (1836) 172.17.8.35 aktiv Erweiterte Konfiguration
eingehend 135 TCP Beschränkt auf IP Generic Host Process for Win32 Services (1388) Alle aktiv (0)
eingehend 123 UDP Beschränkt auf IP Generic Host Process for Win32 Services (1512) 127.0.0.1 aktiv (0)
eingehend 1028 UDP Beschränkt auf IP Generic Host Process for Win32 Services (1512) 127.0.0.1 aktiv (0)
eingehend 1041 UDP Beschränkt auf IP Generic Host Process for Win32 Services (1512) 172.17.8.35 aktiv (0)
eingehend 1042 UDP Beschränkt auf IP Generic Host Process for Win32 Services (1512) 127.0.0.1 aktiv (0)
eingehend 52262 UDP Beschränkt auf IP Generic Host Process for Win32 Services (1512) Alle aktiv (0)
Erklärung des Port-Status:
Geschlossen Eine Anwendung hat diesen Port geöffnet und versucht ihn zu verwenden, aber die Firewall blockiert allen Datenverkehr an diesem Port, sodass er effektiv geschlossen ist.
Sicher Nur Antworten auf gesendete Anfragen sind zulässig, anderer Datenverkehr wird blockiert. Der Port ist vollständig geschützt.
Beschränkt auf LAN Der Port ist nur vom Local Area Network aus zugänglich. Der Port ist vor Zugriffen aus dem Internet vollständig geschützt.
Beschränkt auf IP Der Port ist nur von einer IP (oder einer beschränkten Gruppe von IPs) aus zugänglich. Der Port ist vor Zugriffen aus dem Internet vollständig geschützt.
Offen Der Port ist vom Internet aus zugänglich. Wenn einer oder mehrere Ihrer Ports offen sind, ist Ihr Computer im Internet sichtbar. Nur Server-Software wie beispielsweise Web- und FTP-Server sollten offen sein. Beachten Sie, dass die Firewall den Port nicht schützen kann, wenn er "offen" ist. Er kann jedoch durch eine Anwendung geschützt werden.
Offen (gesichert) Der Port ist vom Internet aus zugänglich, er wird jedoch durch eine Anwendung geschützt.

Ports, die für das Internet geöffnet sind, werden rot angezeigt und erfordern Ihre volle Aufmerksamkeit, denn die Firewall kann einen offenen Port nicht schützen. Die Nutzung offener Ports durch Serversoftware wie FTP- und Webserver ist zulässig. Wenn allerdings eine unbekannte Anwendung einen offenen Port aktiv nutzt, besteht Anlass zur Sorge.

Anwendung anhalten

Um eine Anwendung anzuhalten, markieren Sie einen Eintrag und klicken auf **Anwendung beenden**. Die Anwendung wird sofort beendet, selbst wenn sie noch etwa eine Minute lang in der Liste angezeigt wird.

Eingabe der Option „Erweiterte Konfiguration öffnen"

Markieren Sie einen Eintrag, und wählen Sie die Option **Erweiterte Konfiguration öffnen**.

HINWEIS: Wenn Sie für die Konfiguration einer Anwendung „Verweigern" statt „Zulassen" festlegen möchten, entfernen Sie das Häkchen. Klicken Sie dann auf OK. Wenn einer Anwendung der Zugriff auf das Internet doch gewährt werden soll, setzen Sie ein Häkchen. Beachten Sie, dass „Anwendung beenden" und „Zugeordnete Regel bearbeiten" nur für Einträge gilt, für die eine Regel erstellt wurde. Die Option „Erweiterte Konfiguration öffnen" ist nur für Regeln verfügbar, die unter die „erweiterte Konfiguration" fallen.

Copyright © 1990-2010 Norman ASA

Personal Firewall-Regeln exportieren

Hiermit sichern Sie Ihre Personal Firewall-Regeln. Wählen Sie die Option **Personal Firewall-Regeln exportieren**, und legen Sie einen Speicherort fest. Speichern Sie die Datei auf einem externen Datenträger als Sicherungskopie.

Personal Firewall-Regeln importieren

Hiermit stellen Sie Ihre Personal Firewall-Regeln wieder her. Wählen Sie die Option **Personal Firewall-Regeln importieren**, und geben Sie den Speicherort an, von dem die Sicherungskopie abgerufen werden soll.

Copyright © 1990-2010 Norman ASA

Einstellungen

Personal Firewall konfigurieren

Im Zuge der Installation wurden automatisch mehrere Regeln erstellt, darunter solche für gängige Browser, Mail-Clients, MSN und weitere Programme, die auf das Internet zugreifen müssen.

Gehen Sie nacheinander auf **Personal Firewall > Einstellungen > Personal Firewall konfigurieren**. Um bestehende Regeln anzuzeigen und/oder zu bearbeiten, schlagen Sie bitte den Abschnitt „Regelassistent“ auf Seite 33.

Ausgehende Anwendungen

Unter Umständen greifen auch Anwendungen, für die keine Regeln vorliegen, auf das Internet oder das LAN zu. In diesem Dialogfeld können Sie bestimmen, wie die Personal Firewall mit solchen Anwendungen verfahren soll. Die Standardeinstellung lautet **Eingabeaufforderung**. Nach Aufforderung können Sie beispielsweise die betreffende Anwendung selbst einstufen und eine Regel festlegen. Alternativ können Sie **Verweigern** festlegen, sodass sämtlichen Programmen ohne permanente oder sitzungsbasierte Regel der Netzwerkzugriff verweigert wird.

Serverrechte

Manche Anwendungen ohne Regeln versuchen eventuell, Verbindungen aus dem Internet zuzulassen. In diesem Dialogfeld können Sie bestimmen, wie die Personal Firewall mit solchen Anwendungen verfahren soll. Die Standardeinstellung lautet **Eingabeaufforderung**. Nach Aufforderung können Sie selbst einschätzen, ob die betreffende Anwendung Netzwerkeinladungen annehmen darf. Alternativ können Sie **Verweigern** festlegen, sodass sämtliche Programme ohne permanente oder sitzungsbasierte Regel Netzwerkeinladungen ablehnen.

HINWEIS: Das Dialogfeld „Regel bearbeiten“ enthält eine Option, die Ihnen ermöglicht, einer Anwendung Serverrechte zu gewähren oder zu verweigern. Näheres zum Konzept der Serverrechte finden Sie auch in den Ausführungen zum Thema Regel bearbeiten**.**

Erweiterte Einstellungen

Der technische Charakter dieser Konfigurationsoptionen erfordert ein gewisses Fachwissen, um die Standardeinstellungen zu ändern. Als Faustregel gilt, dass Sie Einstellungen nur dann ändern sollten, wenn Ihnen deren Bedeutung und die Folgen der Änderung bekannt sind. Für den Durchschnittsbenutzer sind die Standardeinstellungen ausreichend.

Nachstehend ist die Option „Personal Firewall-Operation“ beschrieben. Eine ausführlichere Beschreibung aller Optionen finden Sie in den Hilfedateien der Anwendung.

Benutzermodus wechseln (unerfahren/erfahren)

Gehen Sie nacheinander auf **Personal Firewall > Einstellungen > Erweiterte Einstellungen**, und führen Sie dann einen Bildlauf aus bis zum Abschnitt **Personal Firewall-Operation**.

Diese Option ist aktiviert, falls Sie bei der Installation die Option „Erfahrener Benutzer“ gewählt haben. Sollten Sie dagegen „Unerfahrener Benutzer“ angegeben haben, wird automatisch der Regelassistent gestartet. Die beiden Benutzerstufen unterscheiden sich darin, welches Maß an Unterstützung beim Erstellen neuer Regeln oder beim Ändern vorhandener Regeln verfügbar gemacht wird. Nähere Informationen zum Erstellen von Regeln in den unterschiedlichen Modi finden Sie im Abschnitt „Regelassistent“ auf Seite 33.

Copyright © 1990-2010 Norman ASA

Antispam

Öffnen Sie die Anwendung „Security Suite“, und wählen Sie im linken Menü die Option **Antispam** aus. Nähere Informationen zum Öffnen der Anwendung finden Sie im Abschnitt „Erste Schritte“ auf Seite 13, Informationen zu ihrem Zweck und ihrer Funktionsweise im Abschnitt „Antivirus & Antispyware“ auf Seite 5.

Hauptseite

Diese Anwendung schützt vor unerwünschten Werbe- und Massensendungen per E-Mail (sogenanntem „Spam“), die u. U. eine Bedrohung für das System darstellen. In diesem Kapitel erfahren Sie, wie Sie Spamfilter anpassen, Sperr- und Zulassungslisten erstellen, gefilterte E-Mails verwalten und einsehen und Updateintervalle festlegen. Ferner werden Spamverwaltungsoptionen behandelt.

Spamstatistik

Die grafische Ansicht zeigt an, wie viele Spam-Mails und Phishing-Angriffe von der Anwendung in den letzten beiden Wochen pro Tag blockiert wurden.

Einstellungen anpassen

Klicken Sie auf diese Option, um die Standardwerte zu bearbeiten. Nähere Informationen finden Sie im Abschnitt „Einstellungen“ auf Seite 43. Allgemeine Informationen zur Wahl zwischen empfohlenen und benutzerdefinierten Einstellungen finden Sie im Abschnitt „Einstellungen der Security Suite“ auf Seite 15.

Sperren/Zulassen

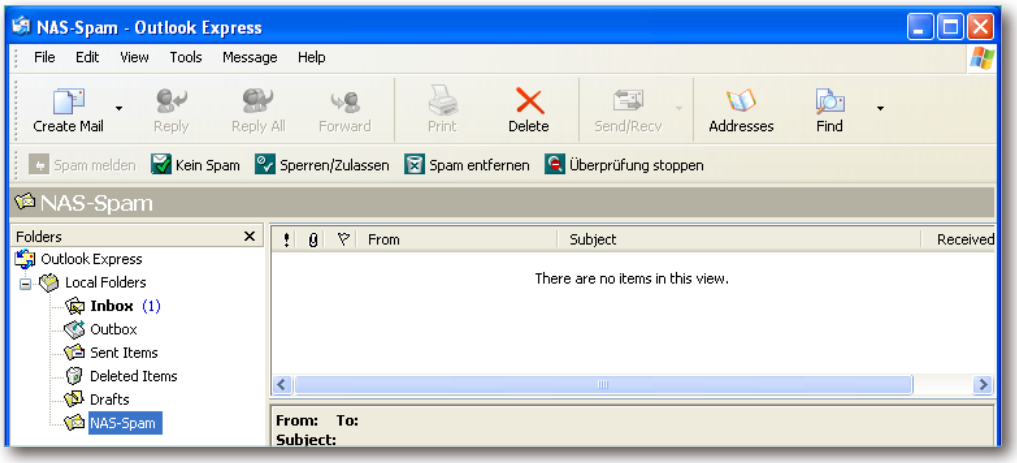
Mithilfe der Sperr-/Zulassungsliste können Sie einzelne E-Mail-Adressen verwalten, um für die Anwendung festzulegen, welche Adressen immer zugelassen bzw. immer abgelehnt werden sollten. Die Antispam-Filtermethode setzt nie Ihre manuellen Anweisungen bezüglich einer Adresse außer Kraft (Sperren bzw. Zulassen). Nähere Informationen finden Sie im Abschnitt „Sperren/Zulassen“ auf Seite 42.

Copyright © 1990-2010 Norman ASA

Gefilterte E-Mail-Nachrichten anzeigen

Hiermit können Sie sich anzeigen lassen, welche E-Mail-Nachrichten beispielsweise aus Microsoft Outlook, Outlook Express oder Windows Mail ausgefiltert wurden. Der NAS-Spamfilter wird im Zuge der Installation der Norman Security Suite erstellt oder wenn Sie einen der vorgenannten E-Mail-Clients installieren und Norman Security Suite auf Ihrem Computer bereits ausgeführt wird.

Öffnen Sie Ihren meistbenutzten E-Mail-Client, und suchen Sie nach dem NAS-Spamfilter und dem Antispam-Anwendungsmenü.



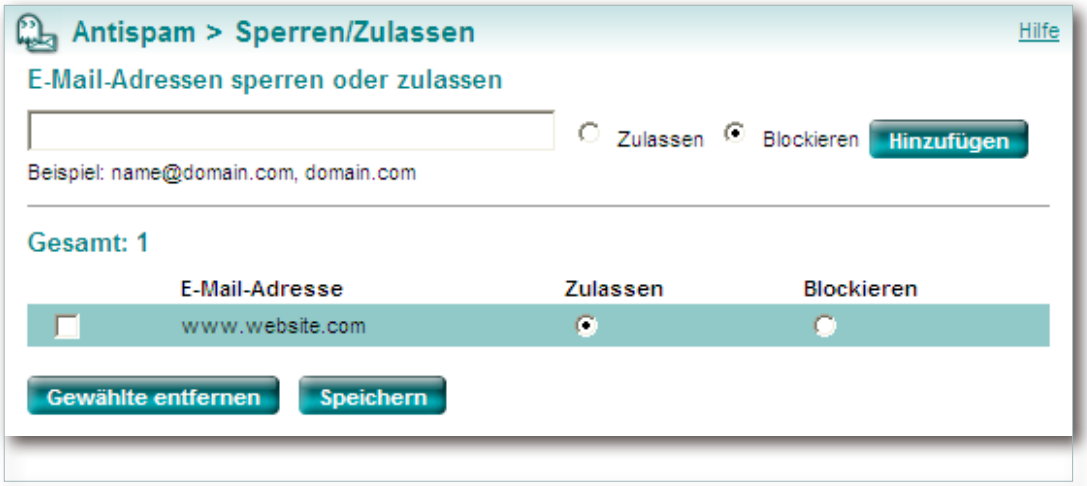
- **Spam melden**
  - Hiermit werden bestimmte E-Mails als Spam gemeldet. Wählen Sie eine E-Mail-Nachricht im Eingangsordner, und klicken Sie in der Symbolleiste auf die Option **Spam melden**. Die Nachricht wird in den Ordner **NAS Spam** verschoben.
- **Kein Spam**
  - Hiermit werden verdächtige E-Mails als zulässig gekennzeichnet. Markieren Sie mindestens eine E-Mail im Ordner **NAS Spam**, und klicken Sie auf **Kein Spam**.
- **Sperren/Zulassen**
  - Hiermit können Sie E-Mail-Adressen sperren oder zulassen Die Auswahl dieser Option öffnet die Anwendung „Norman Antispam“. Geben Sie mindestens eine E-Mail-Adresse ein, und wählen Sie entweder**Sperren** oder **Zulassen**.
- **Spam entfernen**
  - Hiermit löschen Sie den gesamten Inhalt der Ordners **NAS Spam**. Um E-Mails einzeln zu löschen, klicken Sie den betreffenden Eintrag mit der rechten Maustaste an, und wählen Sie im Kontextmenü die Option **Löschen**.
- **Ordner überprüfen**
  - Hiermit prüfen Sie den E-Mail-Eingang auf Spam. Wählen Sie mindestens einen Ordner aus, und klicken Sie auf die Option „Ordner prüfen“, um eine manuelle Prüfung durchzuführen. Diese Option wechselt zwischen **Ordner prüfen** und **Überprüfung stoppen**. Klicken Sie auf **Überprüfung stoppen**, um die Überprüfung auf Spam-Mails anzuhalten.

Nähere Informationen zum automatischen Löschen von Spam finden Sie im Abschnitt „Spamverwaltung“ auf Seite 43.

Copyright © 1990-2010 Norman ASA

Sperren/Zulassen

Hier können Sie E-Mail-Adressen manuell eingeben, die gesperrt oder zugelassen werden sollen. Geben Sie eine E-Mail-Adresse ein, und legen Sie durch Auswahl des betreffenden Optionsfelds fest, ob sie gesperrt oder zugelassen werden soll.



E-Mail-Adresse hinzufügen/entfernen

Im unteren Abschnitt des Dialogfelds ist eine Liste mit E-Mail-Adressen aufgeführt. Beim Eingeben einer neuen Adresse lautet die Standardoption **Sperren**, um die versehentliche Zulassung einer Adresse zu vermeiden, die eigentlich gesperrt sein sollte. Alternativ können Sie aber auch **Zulassen** wählen, wenn Sie E-Mails von diesem Absender empfangen möchten. Die Details in der Liste mit E-Mail-Adressen können Sie jederzeit bearbeiten.

Hinzufügen

1. Geben Sie eine E-Mail-Adresse ein, z. B. `name1@domain.com`.
   oder
   - Geben Sie mehrere durch Komma getrennte E-Mail-Adressen ein, z. B. `name1@domain.com, name2@domain.com`.

   oder
   - Geben Sie den Namen einer ganzen Domäne ein, die gesperrt oder zugelassen werden soll, z. B. `phoneysales.com`.
   - Hinweis: Fügen Sie nicht Ihre eigene Domäne hinzu, um „Spoof"-Mails zu vermeiden.
2. Wählen Sie **Zulassen** oder **Sperren** (Standardoption) für die einzelnen Adressen.
3. Klicken Sie bei jedem neuen Eintrag auf **Hinzufügen**.
4. Klicken Sie auf **Speichern**, um neue Adressen oder Domänen aufzubewahren.

Entfernen

1. Wählen Sie mindestens eine Adresse aus.
2. Klicken Sie auf **Gewählte entfernen**.
3. Klicken Sie auf **Speichern**, um die Änderungen zu bestätigen.

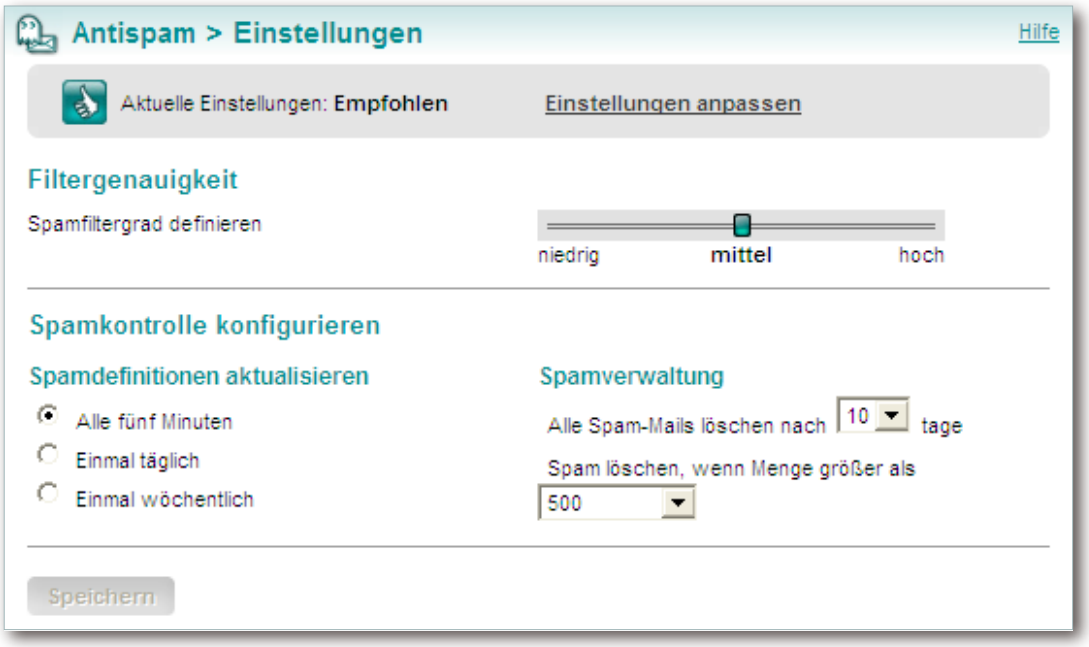
Bearbeiten

1. Wählen Sie mindestens eine Adresse aus.
2. Geben Sie die gewünschten Änderungen für die E-Mail-Adresse ein, die gesperrt bzw. zugelassen werden soll.
3. Klicken Sie auf **Speichern**, um die Änderungen zu bestätigen.

Copyright © 1990-2010 Norman ASA

Einstellungen

So wie Antiviren-Anwendungen mit Virendefinitionsdateien arbeiten, um Malware zu erkennen, verwenden Antispam-Lösungen Definitionsdateien, um unerwünschte E-Mails herauszufiltern. Virendefinitionsdateien nutzen Virensignaturen, um zu ermitteln, ob eine bestimmte Datei infiziert ist, wohingegen Antispam-Definitionen mithilfe eines bestimmten Kriteriensatzes ermitteln, welche E-Mails vermutlich Spam beinhalten. Spam-Definitionen analysieren E-Mails anhand von Sprache, Bildern, Farben, Hyperlinks, die die Mail enthält, sowie anhand der Absender- und IP-Adresse. Trotzdem lässt sich nicht mit letzter Sicherheit sagen, ob es sich bei einer vorliegenden E-Mail um Spam handelt oder nicht.



Filtergenauigkeit

Wenn Sie mithilfe des Schieberegler die Genauigkeit auf **Niedrig** setzen, untersucht die Antispam-Anwendung nur E-Mails, die extrem verdächtig erscheinen. Infolgedessen werden eher weniger E-Mails als Spam aussortiert. Wenn Sie umgekehrt den Schieberegler auf **Hoch** setzen, sorgt eine breitere Auslegung der Spamkriterien entsprechend für eine größere Anzahl von als Spam aussortierten E-Mails.

Wenn so gut wie kein Zweifel besteht, dass es sich bei einer bestimmten E-Mail um Spam handelt, also wenn sich z. B. der Absender auf der Sperrliste oder in einer Online-Datenbank befindet, wird die E-Mail ungeachtet der Stellung des Schiebereglers blockiert. Wir halten die Standardeinstellung **Mittel** für angemessen zum Ausfiltern unerwünschter E-Mails.

Die Antispam-Filtermethode setzt nie Ihre manuellen Anweisungen bezüglich einer Adresse außer Kraft.

Spamkontrolle konfigurieren

Spamdefinitionen aktualisieren

Hiermit wählen Sie die Häufigkeit für die Aktualisierung der Spamdefinitionen, wobei alle fünf Minuten, einmal täglich oder einmal pro Woche zur Auswahl stehen. Die empfohlene Einstellung ist **Alle fünf Minuten**.

Spamverwaltung

Mithilfe dieser Option bestimmen Sie, wann die vom Spamfilter abgefangenen E-Mails gelöscht werden sollen, und zwar je nach Alter oder Anzahl. Die Standardeinstellungen lauten **Alle Spam-Mails löschen nach** [10] **Tagen** und **Spam löschen, wenn Menge größer als** [500] herausgefilterte E-Mail-Nachrichten ist.

Vergessen Sie nicht, Ihre Änderungen zu bestätigen, indem Sie auf **Speichern** klicken.

Copyright © 1990-2010 Norman ASA

Parental Control

Öffnen Sie die Anwendung „Security Suite“, und wählen Sie im linken Menü die Option **Parental Control** aus. Nähere Informationen zum Öffnen der Anwendung finden Sie im Abschnitt „Erste Schritte“ auf Seite 13, Informationen zu ihrem Zweck und ihrer Funktionsweise im Abschnitt „Parental Control“ auf Seite 7.

Ursprünglicher Zugriff

Bevor Sie diese Anwendung zum ersten Mal verwenden, erscheint die Mitteilung *„Administrator nicht erstellt!“* im Start-Dialogfeld, und ein gelbes Warndreieck erscheint auf dem Menüeintrag der Anwendung.

1. **Administrator nicht erstellt**

Sie müssen zunächst einen Benutzer mit Administratorrechten ausstatten, um auf diese Anwendung zuzugreifen. Geben Sie ein Kennwort ein, und wählen Sie das Standardprofil. Klicken Sie auf **Speichern**, um fortzufahren.

Das Standardprofil sollte dem am niedrigsten eingestuften Benutzerprofil entsprechen, das eingerichtet werden soll. Wenn Sie also beispielsweise beabsichtigen, ein Kinderprofil einzurichten, sollte das Grundprofil dem Kinderprofil entsprechen. Nur der Administrator darf in der Lage sein, die Benutzer zu bearbeiten und ihre Einstellungen zu konfigurieren, also etwa das Zeitfenster für den Internetzugriff festzulegen und Sperr-/Zulassungslisten zu erstellen. Normalerweise handelt es sich beim Administrator um ein Elternteil.

Diese Einstellungen können Sie auch später noch über die Option **Parental Control > Einstellungen** ändern.

HINWEIS: Das Administratorkennwort kann nicht zurückgesetzt werden. Achten Sie also darauf, dass Sie Ihr Kennwort nicht vergessen. Beim Kennwort ist die Groß-/Kleinschreibung zu beachten.

2. **Administratoranmeldung**

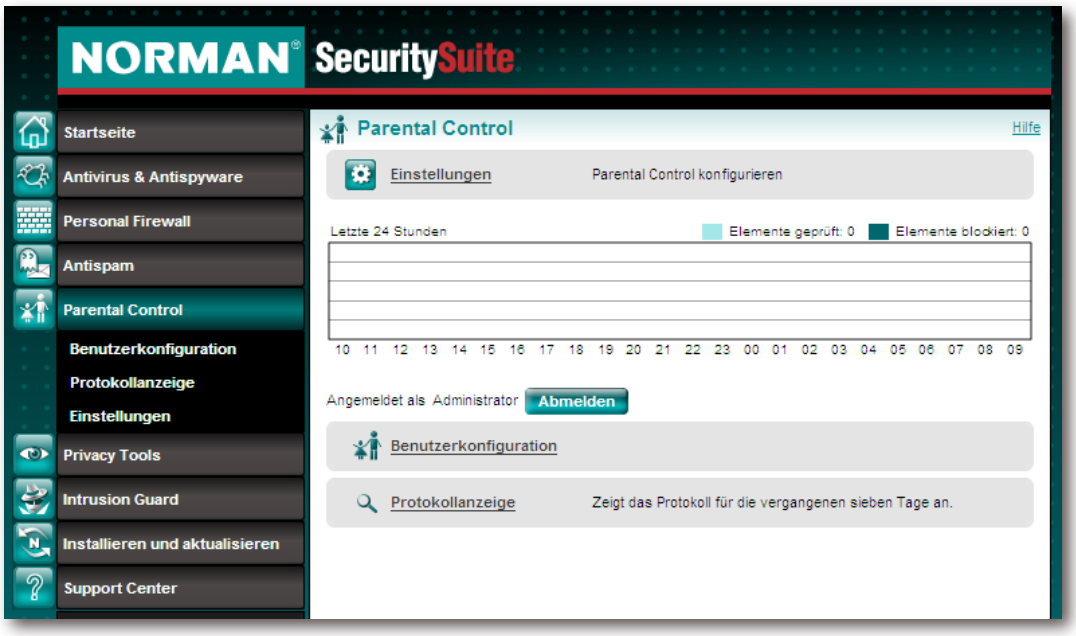
Wenn ein Administratorbenutzer erstellt wird, erscheint der Anmeldungsbildschirm. Melden Sie sich mit dem Benutzernamen und Kennwort des Administrators an, um auf die Anwendung zuzugreifen.

Taskleisten-Symbol

Ein Taskleisten-Symbol zeigt an, dass die Parental Control installiert ist. Wenn Sie mit dem Mauszeiger über das Symbol gehen, wird der Statustext eingeblendet, z. B. „Parental Control: 'Administrator' ist angemeldet“.

Copyright © 1990-2010 Norman ASA

Hauptseite



Diese Anwendung sperrt den Zugang zu Websites bestimmter Kategorien, und es schränkt Umfang und Zeitraum des Internetzugriffs für Benutzer ein. Dieses Kapitel behandelt das Erstellen, Konfigurieren und Verwalten von Benutzern sowie das Anzeigen von Protokolldateien und das Programmieren des Internetzugriffs. Melden Sie sich mit dem Benutzernamen und Kennwort des Administrators an, um auf die Anwendung zuzugreifen.

Einstellungen

Klicken Sie auf diese Option, um die Standardwerte zu bearbeiten. Nähere Informationen finden Sie im Abschnitt „Einstellungen“ von Parental Control auf Seite 50.

Statistik

Auf der Hauptseite können Sie die Statistik für gesperrte und geprüfte Elemente verfolgen.

Benutzerkonfiguration

Nähere Informationen finden Sie im Abschnitt „Benutzerkonfiguration“ auf Seite 46.

Protokollanzeige

Nähere Informationen finden Sie im Abschnitt „Protokollanzeige“ auf Seite 50.

Copyright © 1990-2010 Norman ASA

Benutzerkonfiguration

Hiermit erstellen Sie Benutzer und weisen ihnen Benutzerprofile zu. Bestehende Benutzer werden in diesem Dialogfeld mit Namen und zugeordnetem Profil aufgeführt.

Es gibt drei Benutzerprofile: **Erwachsener**, **Teenager** und **Kind**. Das letztgenannte Profil ist sehr eingeschränkt und gestattet lediglich den Zugriff auf solche Websites, die manuell vom Administrator in die Zulassungsliste eingetragen wurden.

Erwachsener	Keine Einschränkungen.
Teenager	Durch Kategoriefilter eingeschränkter Zugriff.
Kind	Vollständig eingeschränkt.

Kategorien

Kategorien basieren auf einer Vielzahl von Begriffen und Ausdrücken, anhand derer die Anwendung eine Webseite z. B. als vorrangig erotikorientiert erkennen kann. Die Bedingungen selbst können weder eingesehen noch bearbeitet werden. Für das Profil „Teenager“ gibt es vier Kategorien, die den Zugang zu Webseiten mit dem Inhalt **Erotik**, **Glücksspiel**, **Waffen** und **Drogen** sperren. Alle Kategorien sind standardmäßig aktiviert, aber der Administrator kann die Kategorien deaktivieren, die zulässig sein sollen.

Sperr-/Zulassungsliste

Für Benutzer mit dem Profil „Kind“ muss eine Zulassungsliste eingerichtet werden, da nur die Webadressen auf dieser Liste besucht werden können. Für Benutzer mit dem Profil „Teenager“ können optional Sperr- wie Zulassungslisten eingerichtet werden. Nähere Informationen finden Sie in den Abschnitten „Standardprofil ‚Kind‘“ auf Seite 47 und „Standardprofil ‚Teenager‘“ auf Seite 47.

Format der Webadressen

Der technische Begriff für eine Webadresse lautet URL (Uniform Resource Locator). Platzhalterzeichen (*/?) werden in Webadressen nicht unterstützt. Zulässige Formate:

- http://www.newspaper.com
- www.newspaper.com
- newspaper.com

Die Eingabe einer bestimmten Website ermöglicht Ihnen zwar den Zugriff auf die nachgeordnete Domänenebene(n), aber nicht auf die übergeordnete(n) Ebene(n). So würde beispielsweise die Zulassung von www.newspaper.com/kidsstuff keinen Zugriff auf die übergeordnete Ebene www.newspaper.com. Wenn jedoch zeitung.de hinzugefügt wird, sind sämtliche Ebenen dieser Webadresse freigegeben, also etwa news.newspaper.com, cartoon.newspaper.com, usw.

HINWEIS: Wenn ein Benutzer einem Link von einer zugelassenen Seite aus folgt, wird dieses zugelassen, egal wohin der Benutzer weitergeleitet wird. Allerdings ist es nicht möglich, eine weitere Seite zu öffnen, es sei denn, dies ist der weiterleitenden Instanz explizit gestattet.

Copyright © 1990-2010 Norman ASA

Standardprofileinstellungen

Das Profil **Erwachsener** hat keine Einschränkungen. Die Profile **Kind** und **Teenager** unterliegen Einschränkungen, die Sie konfigurieren können. Wenn Sie einem Benutzer das Profil **Kind** zuweisen, hat der Benutzer überhaupt nur Internetzugriff, wenn eine Positivliste zugelassener Websites erstellt wurde. Diese einzelnen Profileinstellungen gelten jeweils für alle Benutzer mit dem betreffenden Benutzerprofil. Informationen zum Konfigurieren eines speziellen Benutzerprofils finden Sie im Abschnitt „Benutzer anlegen“ auf Seite 48.

Standardprofil ‚Kind‘

Bitte beachten Sie, dass Veränderungen an diesem Standardprofil sich auf alle Profilmitglieder auswirken, nicht nur auf einen einzelnen Benutzer. Da für das Profil „Kind“ alle Webseiten blockiert sind, sofern sie nicht ausdrücklich zugelassen werden, gibt es für dieses Profil keine Blockierliste bzw. Kategorie.

Hinzufügen

1. Geben Sie eine Webadresse, die zugelassen werden soll, im Dialogfeld **Adresse zur Liste hinzufügen** ein.
   - Falls Sie mehrere Adressen eingeben, trennen Sie diese durch ein Komma.
2. Klicken Sie bei jedem neuen Eintrag auf **Hinzufügen**.

Entfernen

1. Wählen Sie mindestens eine Adresse aus.
2. Klicken Sie auf **Gewählte entfernen**.

Standardprofil ‚Teenager‘

Bitte beachten Sie, dass Veränderungen an diesem Standardprofil sich auf alle Profilmitglieder auswirken, nicht nur auf einen einzelnen Benutzer. Für dieses Profil werden Websites nach Kategorien und Sperr-/Zulassungsliste eingeschränkt.

Kategorien

Standardmäßig sind alle Kategorien ausgewählt, d. h., Websites mit bestimmten Inhalten werden für das Profil „Teenager“ gemäß diesen Einstellungen gesperrt. Die Kategorien sind Erotik, Glücksspiele, Waffen und Drogen. Der Administrator kann die Kategorien einzeln deaktivieren, um Websites der betreffenden Kategorie zuzulassen. Alternativ können Sie Websites auch auf die Zulassungsliste setzen. Klicken Sie auf **Speichern**, um die Änderungen zu bestätigen.

Copyright © 1990-2010 Norman ASA

Sperr-/Zulassungsliste

Websites für das Profil „Teenager“ werden gemäß den Einstellungen in den Kategorien gesperrt. Sie können eine oder mehrere Websites hinzufügen, um Zugriff auf einzelne Internetseiten zuzulassen, die sonst einer gesperrten Kategorie angehören würden.

Hinzufügen

1. Geben Sie eine Webadresse, die zugelassen werden soll, im Dialogfeld **Adresse zur Liste hinzufügen** ein.
   - Falls Sie mehrere Adressen eingeben, trennen Sie diese durch ein Komma.
2. Klicken Sie bei jedem neuen Eintrag auf **Hinzufügen**.
3. Wählen Sie zwischen den Optionen **Sperren** und **zulassen**.
4. Klicken Sie bei jedem neuen Eintrag auf **Hinzufügen**.

Benutzer anlegen

Wählen Sie die Option **Benutzer anlegen** im Menü **Parental Control > Benutzerkonfiguration**.

1. Geben Sie einen Namen für den neuen Benutzer ein sowie ein Kennwort, das Sie anschließend bestätigen müssen.
2. Der nächste Schritt besteht aus dem **Wählen des Standardprofils** für den neuen Benutzer**.**
   - Mit der Zuordnung eines Profils legen Sie fest, welche Art von Websites der betreffende Benutzer aufrufen kann:
     - Erwachsener
       Keine Einschränkungen. Der Benutzer kann auf alle Websites zugreifen.
     - Teenager
       Grundsätzlich keine Einschränkungen. Allerdings werden Websites mit unerwünschten Themen oder Inhalten durch die Standardeinstellungen der Kategorien gesperrt.
     - Kind
       Nur Zugriff auf die Webseiten, die der Administrator in die Zulassungsliste einträgt.
3. Klicken Sie auf **Speichern**, um Ihre Änderungen zu bestätigen.
   - Bevor Sie auf **Speichern** klicken, um einen neuen Benutzer anzulegen, sollten Sie prüfen, ob das gewählte Profil dem bezeichneten Benutzer auch gerecht wird.

Der neue Benutzer wird zur Benutzerliste hinzugefügt. Klicken Sie auf einen Benutzernamen, um den betreffenden Benutzer zu konfigurieren.

Kennwort ändern

Geben Sie den Benutzernamen und das Kennwort für den neuen Benutzer ein.

Kategorien

Diese Auswahl steht nur für das Benutzerprofil „Teenager“ zur Verfügung. Um eine oder mehrere Kategorien für einen bestimmten Benutzer mit dem Teenager-Profil zuzulassen, deaktivieren Sie das bzw. die entsprechenden Kontrollkästchen. Nähere Informationen finden Sie in den Abschnitten „Kategorien“ auf Seite 46 und „Standardprofil ‚Teenager‘“ auf Seite 47.

Sperr-/Zulassungsliste

Diese Auswahl steht nur für das Benutzerprofil „Teenager“ zur Verfügung. Hier können Sie Webadressen für Benutzer zulassen oder sperren. Nähere Informationen finden Sie in den Abschnitten „Sperr-/Zulassungsliste“ auf Seite 46 und „Standardprofil ‚Teenager‘“ auf Seite 47.

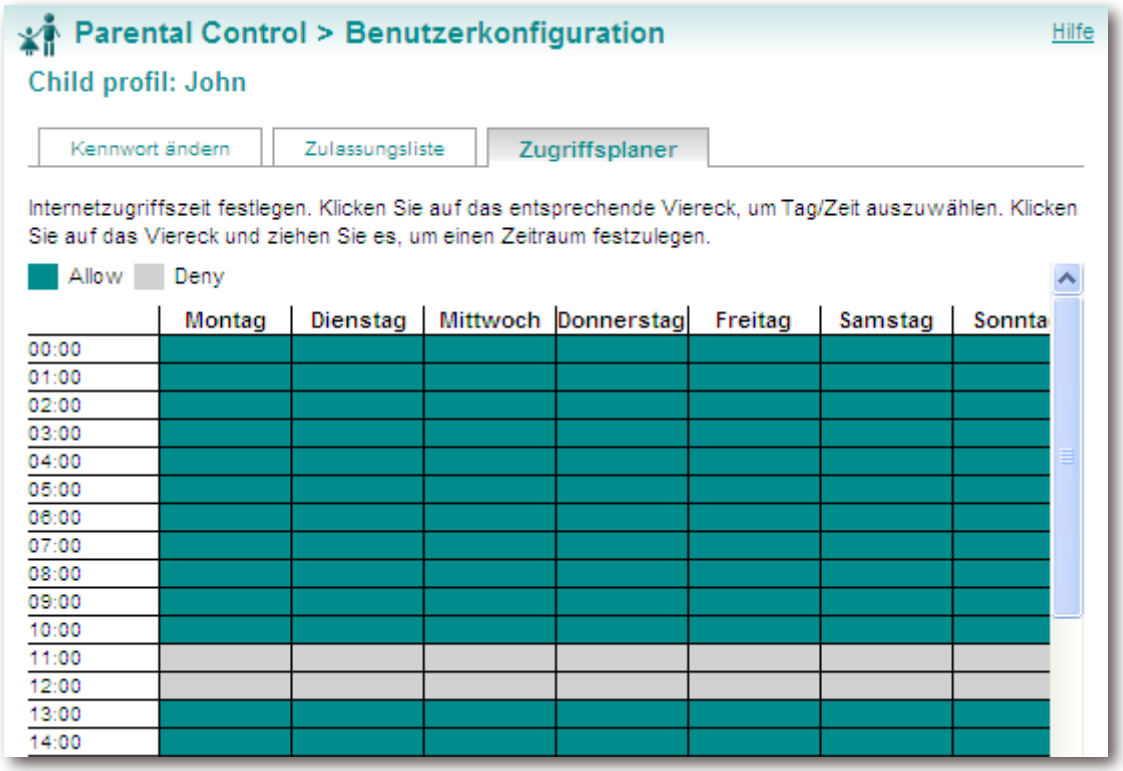
Zulassungsliste

Diese Auswahl steht für das Benutzerprofil „Kind“ zur Verfügung. Hier können Sie Webadressen für Benutzer zulassen. Nähere Informationen finden Sie im Abschnitt „Standardprofil ‚Kind‘“ auf Seite 47.

Copyright © 1990-2010 Norman ASA

Zugriffsplaner

Der Administrator kann entscheiden, zu welcher Tageszeit und an welchen Wochentagen Benutzer im Internet surfen dürfen. Die Standardeinstellung sieht keine zeitlichen Einschränkungen vor (grün).



1. Um den Internetzugriff für einen bestimmten Zeitraum zu sperren, setzen Sie den Cursor auf Tag und Uhrzeit Ihrer Wahl und drücken die linke Maustaste.
2. Wenn Sie den gesperrten Zeitraum erweitern möchten, ziehen Sie den Cursor entsprechend nach oben/unten bzw. nach rechts/links. Analog dazu können Sie den Status durch Klicken und Ziehen des Cursors von **Verweigern** (grau) in **Zulassen** (grün) ändern.
3. Klicken Sie auf **Speichern**, um Ihre Änderungen zu bestätigen.

Copyright © 1990-2010 Norman ASA

Protokollanzeige

Die Anwendung protokolliert automatisch die Websites, die für Benutzer mit den Profilen „Teenager“ und „Kind“ gesperrt sind. Die Protokolle zeigen nicht an, welche Seiten ein bestimmter Benutzer besucht hat.

Das Protokoll zeigt gesperrte Seiten bis zu einer Woche lang an. Es gibt für jeden Wochentag ein Protokoll, sodass Sie einen Wochentag wählen müssen anstatt eines Datums. Die Anwendung schlägt den aktuellen Wochentag als Standard vor.

Die Spalten im Protokoll zeigen Datum, Uhrzeit, Benutzer, Grund der Sperre und die gesperrte URL an.

Falls die Spalte „Benutzer“ leer ist, befand sich das System im Fallback-Modus, ohne dass ein Benutzer angemeldet war.

Einstellungen

Sie können auch vermeiden, dass ein Kind auf einen unbeaufsichtigten Computer zugreift, auf dem ein Erwachsener angemeldet ist (und vergessen hat, sich abzumelden, oder den Computer plötzlich verlassen musste). Nach einer festgelegten Leerlaufzeit wechselt der Computer in das Standardprofil.

Wartezeit vor Wechsel zu Standardprofil

Die Dauer der Nichtbenutzung ist als der Zeitraum definiert, in dem das System keine Aktivitäten verzeichnet, d. h. keine Eingaben über die Tastatur oder Maus.

- Wählen Sie im Dropdown-Menü den Zeitraum aus, nach welchem die Anwendung bei Leerlauf des Computers in das Standardprofil zurückgesetzt werden sollte.
- Klicken Sie auf **Speichern**, um Ihre Änderungen zu bestätigen.

Standardprofil festlegen

Als Profil, in das die Anwendung nach der festgelegten Dauer zurückgesetzt werden soll, können Sie „Kind“ oder „Teenager“ angeben.

- **Kind**
  Alle Webseiten außer der manuell eingegebenen werden für das Profil „Kind“ gesperrt. Dies bedeutet, dass der Internetzugriff überhaupt erst möglich ist, wenn Sie eine Positivliste von Websites für das Benutzerprofil „Kind“ festgelegt haben.
- **Teenager**
  Webseiten mit bestimmten Inhalten sind gemäß den Einstellungen unter „Kategorien“ (Erotik, Glücksspiel, Waffen und Drogen) für das Profil „Teenager“ gesperrt.
- Klicken Sie auf **Speichern**, um Ihre Änderungen zu bestätigen.

Administratorkennwort ändern

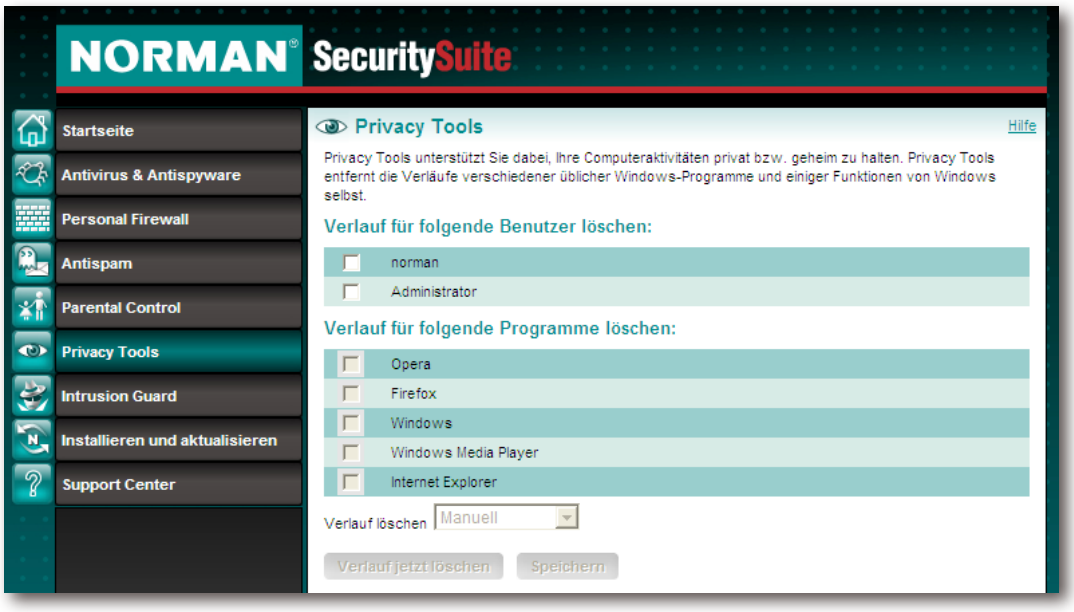
Das Administratorkennwort kann zwar nicht zurückgesetzt, aber geändert werden, sofern Ihnen das aktuelle Kennwort bekannt ist. Wenn Sie ein neues Administratorkennwort festlegen, schreiben Sie es am besten auf und verwahren es an einem sicheren Ort.

HINWEIS: Achten Sie beim Kennwort auf die Groß-/Kleinschreibung.

Copyright © 1990-2010 Norman ASA

Privacy Tools

Öffnen Sie die Anwendung „Security Suite“, und wählen Sie im linken Menü die Option **Privacy Tools** aus. Nähere Informationen zum Öffnen der Anwendung finden Sie im Abschnitt „Erste Schritte“ auf Seite 13, Informationen zu ihrem Zweck und ihrer Funktionsweise im Abschnitt „Privacy Tools“ auf Seite 7.



Mithilfe dieser Anwendung können Sie bestimmte Dateien sicher löschen. Die Inhalte solcher Dateien sind dauerhaft gelöscht und lassen sich nicht wiederherstellen. Sie können die Anwendung auch so konfigurieren, dass diverse Protokolldateien mit persönlichen Daten, Cookies und Browserverläufen automatisch gelöscht werden. Das Löschen von Verlaufsprotokollen wirkt sich nicht auf die Einstellungen und Lesezeichen einer Anwendung aus.

Programmverlauf eines Benutzers löschen

Die Liste der Benutzernamen zeigt alle registrierten Benutzer des betreffenden Computers an, und die Programmliste zeigt alle Anwendungen an, deren Verlaufsprotokolle Sie löschen können.

- Wählen Sie mindestens einen Benutzernamen sowie die Programme aus, deren Verläufe gelöscht werden sollen.
- Klicken Sie zum Bestätigen auf **Verlauf jetzt löschen**.

Verlauf manuell oder automatisch löschen

Sie können die Verlaufsprotokolle wahlweise manuell löschen oder die Anwendung so konfigurieren, dass sie automatisch in festgelegten Abständen gelöscht werden.

- **Manuell**.
  Verlaufsprotokolle werden erst gelöscht, wenn Sie auf **Verlauf jetzt löschen** klicken.
- **Alle 10 Minuten** oder **Jede Stunde**.
  Verlaufsprotokolle werden automatisch in den festgelegten Zeitabständen gelöscht.
- Klicken Sie auf **Speichern**, um Ihre Änderungen zu bestätigen.

HINWEIS: Falls Sie festlegen, dass der Verlauf Manuell **gelöscht werden soll, werden die Protokolle erst gelöscht, nachdem Sie** Verlauf jetzt löschen **angeklickt haben. Sie werden NICHT AUTOMATISCH gelöscht.**

Copyright © 1990-2010 Norman ASA

Sicher löschen

Mithilfe dieser Anwendung können Sie bestimmte Dateien sicher löschen. Die Inhalte solcher Dateien sind dauerhaft gelöscht und lassen sich nicht wiederherstellen.

Sie können den Vorgang zum sicheren Löschen von Dateien einleiten, indem Sie einfach mit der rechten Maustaste die betreffende Datei anklicken. Sie werden aufgefordert, den Löschvorgang zu bestätigen. Der Löschvorgang wird angezeigt, und nach seinem Abschluss erscheint eine Zusammenfassung. Verfahren Sie folgendermaßen, um Dateien sicher zu löschen:

- Wählen Sie mindestens eine Datei aus, die gelöscht werden soll.
- Klicken Sie mit der rechten Maustaste die Datei(en) an.
- Wählen Sie im Popup-Menü die Option **Norman Secure Delete** aus.
- Klicken Sie zum Bestätigen auf **OK**.
- Klicken Sie auf **OK**, um das Dialogfeld „Zusammenfassung“ zu schließen.

Damit sind die betreffenden Dateiinhalte dauerhaft von Ihrem Computer gelöscht.

HINWEIS: Das Löschen von Dateien über die sichere Methode ist sehr viel zeitaufwendiger als das normale Löschen von Dateien. Dies liegt daran, dass jeder Dateiteil mehrfach überschrieben wird, um zu verhindern, dass Fragmente der ursprünglichen Inhalte wiederhergestellt werden können.

Falls Sie den Löschvorgang vorzeitig abbrechen, wird die Datei zwar trotzdem vernichtet, aber nicht so gründlich wie vorgesehen.

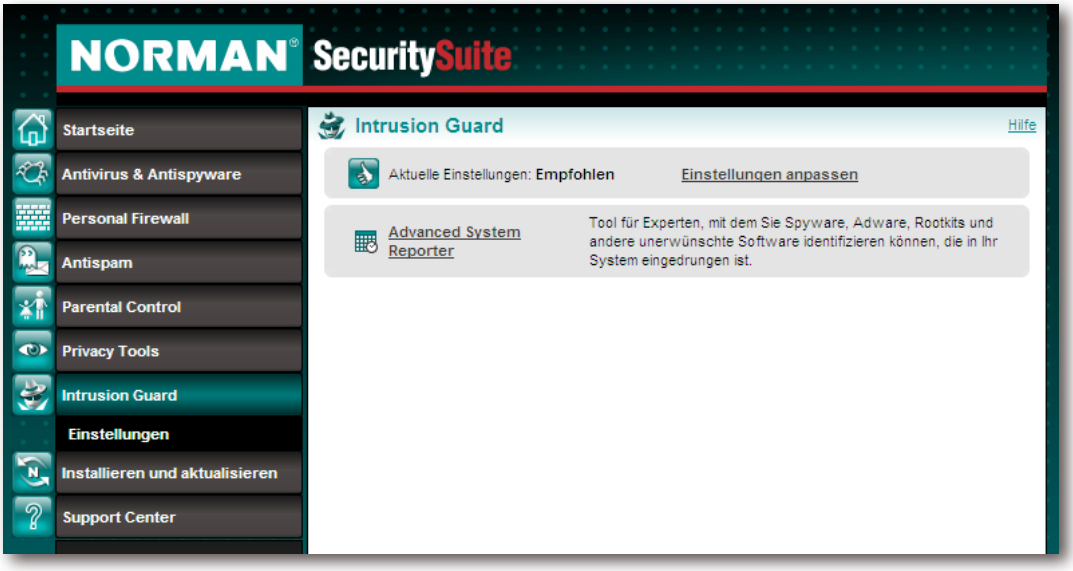
Nicht alle Dateien lassen sich löschen. Das liegt entweder daran, dass der Benutzer nicht die erforderlichen Rechte zum Überschreiben der Datei(en) hat oder es sich um geschützte Systemdateien handelt, die von Secure Delete nicht gelöscht werden können.

Copyright © 1990-2010 Norman ASA

Intrusion Guard

Öffnen Sie die Anwendung „Security Suite“, und wählen Sie im linken Menü die Option **Intrusion Guard** aus. Nähere Informationen zum Öffnen der Anwendung finden Sie im Abschnitt „Erste Schritte“ auf Seite 13, Informationen zu ihrem Zweck und ihrer Funktionsweise im Abschnitt „Intrusion Guard“ auf Seite 8.

Hauptseite



Bei dieser Anwendung handelt es sich um ein hostbasiertes Angriffsverteidigungssystem (HIPS) für erfahrene Benutzer. Unerfahrene Benutzer sollten die empfohlenen Konfigurationseinstellungen unverändert beibehalten, die hauptsächlich dem Zulassen und Protokollieren von Ereignissen dienen. Hochriskante Ereignisse, die von zulässigen Anwendungen kaum verwendet werden, sind standardmäßig gesperrt.

Einstellungen anpassen

Klicken Sie auf diese Option, um die Standardwerte zu bearbeiten. Nähere Informationen finden Sie im Abschnitt „Einstellungen“ auf Seite 53. Allgemeine Informationen zur Wahl zwischen empfohlenen und benutzerdefinierten Einstellungen finden Sie im Abschnitt „Einstellungen der Security Suite“ auf Seite 15. Wir empfehlen, dass nur fortgeschrittene Benutzer diese Einstellungen verändern (d. h. die Standardeinstellungen).

Advanced System Reporter

Dieses Werkzeug ist für erfahrene Benutzer gedacht. Es erkennt unbekannte Spyware und Rootkits, indem es Ihren Computer nach ungewöhnlichen Vorgängen absucht. Nähere Informationen finden Sie im „Anhang B“ auf Seite 64.

Einstellungen

In diesem Dialogfeld können Sie die Konfiguration der Anwendung einsehen und bearbeiten. Wählen Sie im obersten Teil des Dialogfelds die Option **Einstellungen anpassen**, um die Standardeinstellungen zu ändern, oder wählen Sie **Empfohlene Einstellungen**, um zu den Standardeinstellungen zurückzukehren.

HINWEIS: Es wird dringend empfohlen, dass nur fortgeschrittene Benutzer die Standardeinstellungen ändern.

Copyright © 1990-2010 Norman ASA

Treiber und Speicher

Intrusion Guard > Einstellungen
Hilfe
Aktuelle Einstellungen: Empfohlen
Einstellungen anpassen
Treiber und Speicher
Prozesse
Netzwerk
Treiberinstallation
Systemtreiber können auf Hardwaregeräte zugreifen und diese steuern. Damit das möglich ist, werden ihnen Rechte für den vollständigen Systemzugriff eingeräumt, die noch umfangreicher sind als die von Anwendungen mit Administratorrechten. Was soll Intrusion Guard tun, wenn eine Anwendung versucht, Treiber auf Ihrem System zu installieren?
Eingabeaufforderung
Zulassen
Verweigern
Zugriff auf physischen Speicher (nur 32-Bit)
Durch die direkte Veränderung des physischen Speichers kann eine Anwendung Aufgaben ausführen, die normalerweise durch das Betriebssystem geschützt sind. Was soll Intrusion Guard tun, wenn eine Anwendung versucht, auf den physischen Speicher zuzugreifen?
Eingabeaufforderung
Zulassen
Verweigern
Treiber laden und ausführen (nur 32-Bit)
Eine schädliche Anwendung kann versuchen, einen Systemtreiber zu laden, ohne ihn vorher zu installieren. Was soll Intrusion Guard tun, wenn eine Anwendung versucht, Treiber direkt zu laden und auszuführen?
Speichern

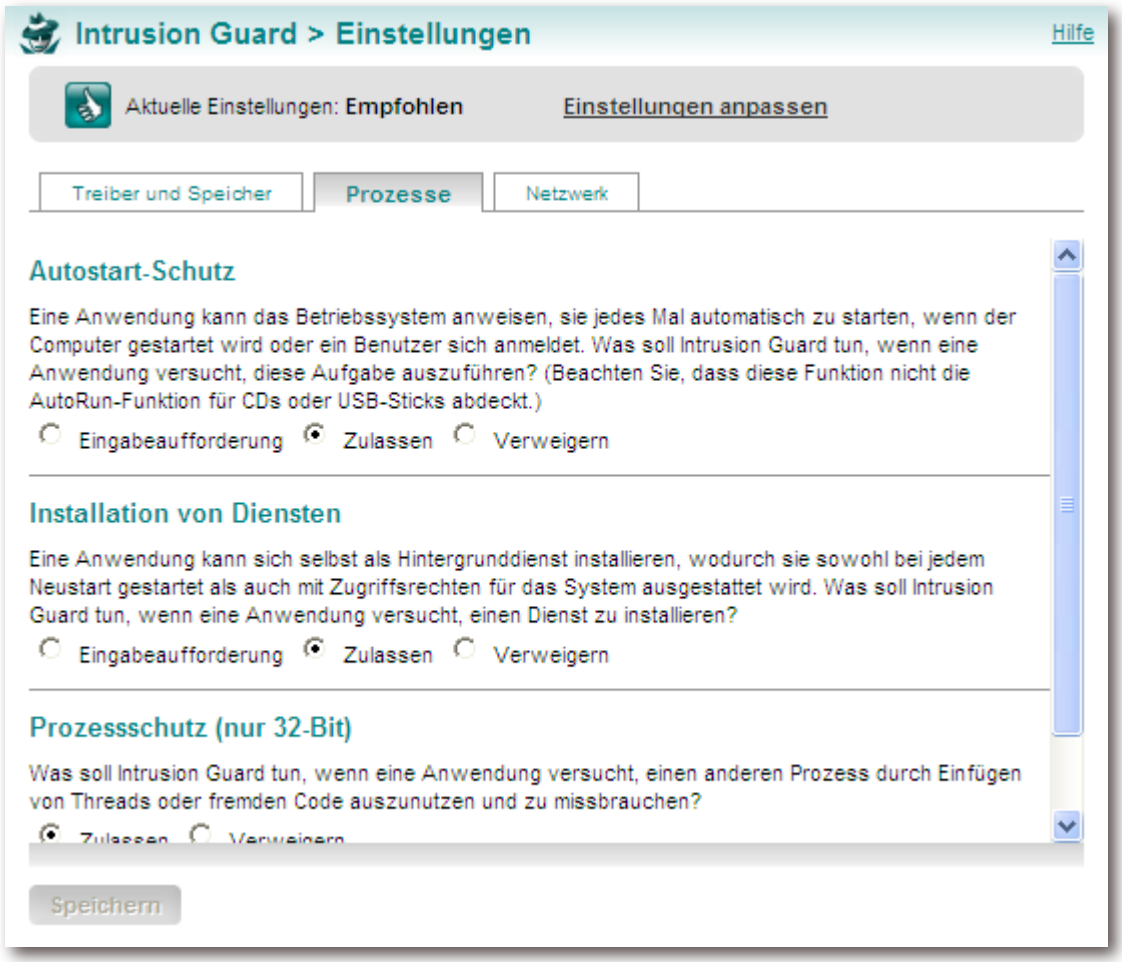
Treiber sind Computerprogramme, die auf einer unteren Ebene ausgeführt werden, der „Kernel-Ebene“. Treiber werden normalerweise für den Zugriff und die Steuerung von Hardware geschrieben, z. B. Monitor, Tastatur, Drucker und Netzwerkkarte. Um auf die an den Computer angeschlossene Hardware zuzugreifen, benötigen Treiber uneingeschränkten Systemzugriff. Daher kommen beim Schreiben bösartiger Anwendungen die gleichen Methoden zum Einsatz. Sie können die Konfiguration der Treiberinstallation ändern, um zu steuern, welche Anwendungen Treiber auf Ihrem Computer installieren dürfen.

Es gibt zwei bösartige Methoden, um die gleichen Rechte wie Treiber zu erlangen. Beide Methoden umgehen den Sicherheitsmechanismus des Betriebssystems. Es wird dringend empfohlen, die Einstellungen in beiden Fällen auf **Verweigern** zu belassen.

- **Eingabeaufforderung**
  Sie werden bei jedem Versuch zum Bestätigen aufgefordert.
- **Zulassen**
  Versuche werden nur protokolliert.
- **Verweigern**
  Keine Anwendung, ob berechtigt oder bösartig, kann Treiber auf der Kernel-Ebene installieren.

Copyright © 1990-2010 Norman ASA

Prozesse


Intrusion Guard > Einstellungen
Hilfe
Aktuelle Einstellungen: Empfohlen
Einstellungen anpassen
Treiber und Speicher
Prozesse
Netzwerk
Autostart-Schutz
Eine Anwendung kann das Betriebssystem anweisen, sie jedes Mal automatisch zu starten, wenn der Computer gestartet wird oder ein Benutzer sich anmeldet. Was soll Intrusion Guard tun, wenn eine Anwendung versucht, diese Aufgabe auszuführen? (Beachten Sie, dass diese Funktion nicht die AutoRun-Funktion für CDs oder USB-Sticks abdeckt.)
Eingabeaufforderung
Zulassen
Verweigern
Installation von Diensten
Eine Anwendung kann sich selbst als Hintergrunddienst installieren, wodurch sie sowohl bei jedem Neustart gestartet als auch mit Zugriffsrechten für das System ausgestattet wird. Was soll Intrusion Guard tun, wenn eine Anwendung versucht, einen Dienst zu installieren?
Eingabeaufforderung
Zulassen
Verweigern
Prozessschutz (nur 32-Bit)
Was soll Intrusion Guard tun, wenn eine Anwendung versucht, einen anderen Prozess durch Einfügen von Threads oder fremden Code auszunutzen und zu missbrauchen?
Zulassen
Verweigern
Speichern

Eine auf Ihrem Computer installierte Anwendung – egal ob legitim oder bösartig – wird meist versuchen, automatisch zu starten, sobald der Computer hochfährt. Ein Programm, das automatisch zu starten versucht, kann das Betriebssystem anweisen, automatisch mit den gleichen Rechten wie der aktuelle Benutzer zu starten, wenn der Computer hochfährt. Oder es kann einen Hintergrunddienst installieren, der mit erhöhten Zugriffsrechten ausgeführt wird. Eine Angriffsverteidigungsanwendung kann Zugriffsversuche dieser Art verhindern.

- **Eingabeaufforderung**
  Sie werden bei jedem Versuch zum Bestätigen aufgefordert.
- **Verweigern**
  Keine Anwendung, ob berechtigt oder bösartig, kann automatisch starten, wenn der Computer hochfährt.

Programme können auch Code in andere Prozesse einschleusen, die auf Ihrem Computer ausgeführt werden, oder Prozesse auf andere Weise missbrauchen. Es handelt sich um das normale Verhalten von bösartigen Anwendungen, allerdings verwenden auch bestimmte zulässige Programme diese Methoden, etwa um das Benutzerdesktop to erweitern oder sonstige erweiterte Funktionen des Betriebssystems oder von Drittanwendungen bereitzustellen. Sie können die Anwendung so konfigurieren, dass jeglicher Versuch verweigert oder Ihnen zur Bestätigung vorgelegt wird.

Sie können eine Liste vertrauenswürdiger Anwendungen so bearbeiten, dass sie zulässige Anwendungen mit ähnlichem Verhalten beinhalten.

Copyright © 1990-2010 Norman ASA

Netzwerk

Intrusion Guard > Einstellungen
Hilfe
Aktuelle Einstellungen: Empfohlen
Einstellungen anpassen
Treiber und Speicher
Prozesse
Netzwerk
Schutz vor IE-Plug-Ins
Plug-Ins für Internet Explorer, z. B. Browser-Hilfsprogrammobjekte und Symbolleistenerweiterungen, können die von Ihrem Browser gesendeten und empfangenen Daten verändern und ausspionieren. Was soll Intrusion Guard tun, wenn eine Anwendung versucht, ein Plug-In für Internet Explorer zu installieren?
Eingabeaufforderung
Zulassen
Verweigern
Schutz vor LSPs
Ein LSP (Layered Service Provider) ist ein allgemeiner Netzwerkfilter, der die gesendeten und empfangenen Daten aller Anwendungen auf Ihrem Computer ausspionieren oder verändern kann. Was soll Intrusion Guard tun, wenn eine Anwendung versucht, einen LSP zu installieren?
Eingabeaufforderung
Zulassen
Verweigern
Schutz der Datei "Hosts"
Wenn Sie eine Website mittels des Domain-Namens (der "Webadresse") aufrufen, wird dieser zunächst in eine IP-Adresse übersetzt, ehe mit dem entfernten Server Daten ausgetauscht werden. Ihr Computer schlägt dabei zunächst den Domain-Namen in der Datei "HOSTS" nach, was bedeutet, dass dort vorhandene Einträge jede IP-Adresse überschreiben, die für den Namen geliefert wird. Was soll Intrusion
Speichern

Indem Sie Filter zu Netzwerkmodulen in Ihrem Betriebssystem hinzufügen, können bösartige Anwendungen persönliche Daten stehlen, z. B. Sozialversicherungsnummern, Kreditkartenangaben und Kennwörter. Adware kann die Netzwerkdaten verändern, die durch solche Filter gesendet werden. So lassen sich die Ergebnisse von Suchmaschinen manipulieren, sodass auf Ihrem Desktop oder auf den von Ihnen besuchten Websites unerwünschte Werbung erscheint.

Unter einem BHO (Browser Helper Object) versteht man eine Erweiterung des Microsoft Internet Explorers. Diese und andere Arten von Plug-ins für den Internet Explorer, z. B. Systemleisten, haben volle Kontrolle über den Netzwerkverkehr zum und vom Internet Explorer, und sie interagieren mit der Benutzeroberfläche.

Bei einem LSP (Layered Service Provider) handelt sich um einen generischen Filter im Netzwerkstapel in Windows. Er hat vollständige Kontrolle über sämtlichen Netzwerkverkehr auf Ihrem Computer.

Wenn Sie eine Website mittels des Domain-Namens (der "Webadresse") aufrufen, wird dieser zunächst in eine IP-Adresse übersetzt. Anschließend werden mit dem entfernten Server Daten ausgetauscht. Ihr Computer schlägt dabei zunächst den Domain-Namen in der Datei „HOSTS“ nach. Dies bedeutet, dass dort vorhandene Einträge jede IP-Adresse überschreiben, die für den Namen geliefert wird. Bösartige Anwendungen können die Datei „HOSTS“ ändern und somit den Netzwerkverkehr auf eine bösartige Website umleiten (sogenanntes „Pharming“).

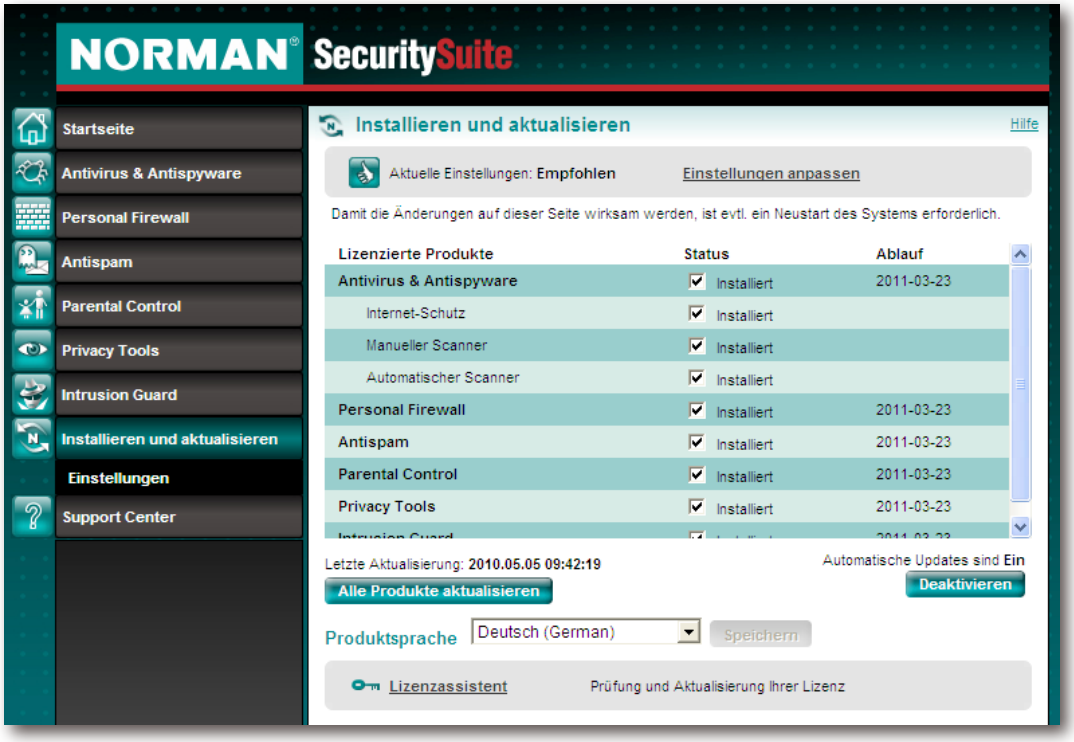
- **Eingabeaufforderung**
  Sie werden bei jedem Versuch aufgefordert zu bestätigen.
- **Verweigern**
  Es werden alle Versuche unterbunden, Ihr System zu ändern und ein BHO oder einen LSP zu installieren.

Copyright © 1990-2010 Norman ASA

Installieren und aktualisieren

Öffnen Sie die Anwendung „Security Suite“, und wählen Sie im linken Menü die Option **Installieren und aktualisieren** aus. Näheres zum Öffnen der Anwendung erfahren Sie im Abschnitt „Erste Schritte“ auf Seite 13.

Hauptseite



Das Menü **Installieren und aktualisieren** zeigt u. a. eine Liste aller in der Security Suite verfügbaren Produkte an. In diesem Menü können Sie Produkte hinzufügen oder entfernen, Updates initiieren, den Lizenzassistenten aktivieren und die Installationssprache der Norman Security Suite ändern.

HINWEIS: Damit die Änderungen auf dieser Seite wirksam werden, ist evtl. ein Neustart des Systems erforderlich.

Einstellungen anpassen

Klicken Sie auf diese Option, um die Standardwerte zu bearbeiten. Nähere Informationen finden Sie im Abschnitt „Einstellungen“ auf Seite 58. Allgemeine Informationen zur Wahl zwischen empfohlenen und benutzerdefinierten Einstellungen finden Sie im Abschnitt „Einstellungen der Security Suite“ auf Seite 15.

Lizenzierte Produkte

Die Liste der lizenzierten Produkte zeigt an, welche Produkte installiert sind und wann die Lizenzen ablaufen. Auf dieser Seite können Sie Produkte oder Komponenten der Liste hinzufügen oder aus der Liste entfernen. Wenn Sie ein Kontrollkästchen deaktivieren, wird das entsprechende Produkt komplett deinstalliert. Wenn Norman Security Suite um neue Produkte/Komponenten erweitert wird, werden diese automatisch heruntergeladen. Alle ausgewählten Produkte werden über die Internet Updatefunktion von Norman Security Suite automatisch aktualisiert.

HINWEIS: Wenn Sie das Kontrollkästchen eines Produkts deaktivieren, wird das deaktivierte Produkt deinstalliert und nicht mehr aktualisiert.

Copyright © 1990-2010 Norman ASA

Alle Produkte aktualisieren

Virendefinitions- und Programmdateien werden häufig aktualisiert. Die Aktualisierung erfolgt über das Internet oder das interne Netzwerk. Sobald Internet Update ein Paket heruntergeladen hat, wird das eigentliche Update automatisch installiert. Nach einem Update fordert das Programm Sie möglicherweise auf, den Computer neu zu starten.

- Klicken Sie einmal auf **Alle Produkte aktualisieren**, um die gesamte Security Suite zu aktualisieren.

Automatische Updates aktivieren/deaktivieren

Standardmäßig sind die automatischen Updates eingeschaltet. Das bedeutet, dass die Produktinstallation immer dann aktualisiert werden, wenn neue Komponenten oder Definitionsdateien dafür vorliegen. Nähere Informationen zu den automatischen Aktualisierungseinstellungen finden Sie im Abschnitt **Einstellungen> Aktualisierungsmethode auswählen**.

HINWEIS: Antivirenprogramme müssen oft aktualisiert werden, um Malware verlässlich erkennen und entfernen zu können.

Produktsprache auswählen

Sie können die im Zuge der Installation gewählte Sprache ändern. Wählen Sie im Dropdown-Menü **Produktsprache** die gewünschte Sprache, und klicken Sie auf **Speichern**. Die Änderungen werden mit der nächsten Aktualisierung wirksam.

Lizenzassistent

Der Lizenzassistent prüft und aktualisiert die Lizenz. Wenn Sie diese Option wählen, erscheint ein Dialog mit Informationen zu den installierten Produkten und Lizenzschlüsselinformationen. Sie benötigen einen gültigen Schlüssel, um die Installation zu aktualisieren.

Einstellungen

Aktualisierungsmethode auswählen

Diese Option ermöglicht Ihnen, zwischen manueller und automatischer Aktualisierung zu wählen. Wir empfehlen die automatische Aktualisierungsmethode, da es extrem wichtig ist, die Software jederzeit auf dem neuesten Stand zu haben.

Copyright © 1990-2010 Norman ASA

Manuell aktualisieren

Wählen Sie diese Option, wenn Sie Internet Update lieber manuell auf der Hauptseite „Installieren und aktualisieren“ („Alle Produkte aktualisieren“) auf den neuesten Stand bringen. Alternativ können Sie Internet Update aus dem Taskleistenmenü starten.

HINWEIS: Die Option Manuell aktualisieren erfordert einen erzwungenen Start der Funktion Internet Update. Die Auswahl dieser Option bedeutet, dass das System NICHT automatisch aktualisiert wird. Es wird dringend empfohlen, die Software häufig zu aktualisieren. Für den Alltag ist das manuelle Aktualisieren nicht geeignet, denn es wird über dem Alltagsgeschäft leicht vergessen.

Automatische Aktualisierung in festen Intervallen

Wählen Sie diese Option, damit das Programm sich automatisch um Downloads und Updates kümmert. Wählen Sie ein zeitliches Intervall in der Liste neben der Option **Automatisch alle**, um das gewünschte Intervall festzulegen. Diese Option setzt eine dauerhafte Internetverbindung voraus.

HINWEIS: Die Option Automatische Aktualisierung in festen Intervallen bedeutet, dass das System automatisch aktualisiert wird. Diese Option ist die empfohlene Aktualisierungseinstellung. Wenn in den letzten 24 Stunden kein Internet-Update erfolgt ist, sucht das Programm beim Start automatisch nach Updates.

Warten auf Wählverbindung (nur für DFÜ-Einwählverbindungen)

Falls Sie sich über ein Modem ins Internet einwählen, verwenden Sie diese Option, um den Produktserver täglich auf Aktualisierungen zu überprüfen. Sie wählen sich dann wie gewohnt ins Internet ein. Das Programm prüft nach der Einwahl, ob aktualisierte Dateien zur Verfügung stehen. Falls Sie täglich mehrmals eine Verbindung zum Internet herstellen, wird nur beim ersten Verbindungsaufbau nach Updates gesucht. Falls Sie sich nur einmal wöchentlich im Internet anmelden, prüft das Programm den Server sofort nach dem Verbindungsaufbau.

Proxy-Einstellungen

Ein Proxy-Server ist ein Computer, der zwischen den Computer des Benutzers und das Internet geschaltet ist. Dieser kann dazu dienen, die Internetnutzung zu protokollieren und den Zugriff auf bestimmte Websites zu sperren. Ferner kann die Firewall des Proxy-Servers dazu verwendet werden, den Zugriff auf bestimmte Seiten von Websites zu sperren.

Falls Ihr Computer von einer Firewall oder einem Proxy-Server geschützt wird, müssen Sie die notwendigen Proxy-Informationen eingeben.

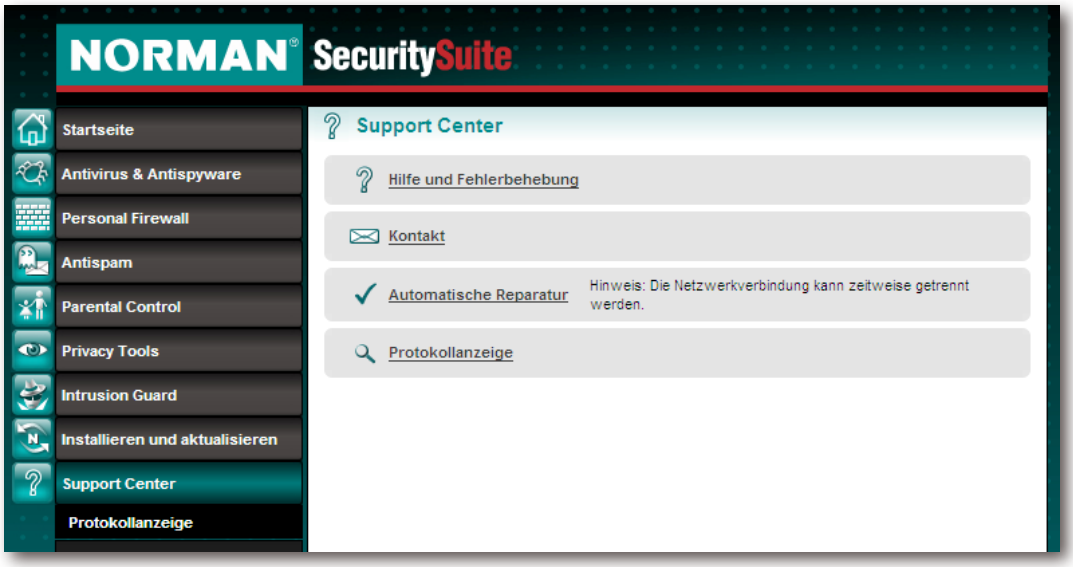
- Gehen Sie nacheinander auf **Installieren und aktualisieren > Einstellungen > Proxy-Einstellungen**.
- Wählen Sie **Proxy-Server verwenden**, und geben Sie eine Proxy-Adresse und den Port ein.
- Wählen Sie **Anmeldeinformationen für den Proxyserver**, und geben Sie Benutzernamen, Kennwort und ggf. Domäne ein (bei Windows NT Challenge/Responses).
  - Windows Challenge/Response Authentication ist das für die Verbindung zu Windows 2000 Server oder Exchange verwendete Format.
  - Das Benutzerkonto hat das folgende Format: [*NT/2000Domänenname*]\[*Kontoname*]

Copyright © 1990-2010 Norman ASA

Support Center

Öffnen Sie die Anwendung „Security Suite“, und wählen Sie im linken Menü die Option **Support Center** aus. Näheres zum Öffnen der Anwendung erfahren Sie im Abschnitt „Erste Schritte“ auf Seite 13.

Hauptseite



Das **Support Center** liefert Informationen, wo Sie weitergehende Hilfe erhalten, als sie die Produktdokumentation und Onlinehilfe bietet. Ferner finden Sie hier eine automatische Reparaturfunktion, die nützlich sein kann, falls Probleme mit der installierten Software auftreten.

Hilfe und Fehlerbehebung

Wenn Sie auf den Link **Hilfe und Fehlerbehebung** klicken, rufen Sie die Website von Norman auf. Dort finden Sie eine Vielzahl hilfreicher Materialien, die Ihnen in den meisten Fällen helfen werden. So finden sie auf dieser Website z. B.:

- Support
- Security Center
- **das Support Forum von Norman**

Wenn auch das Durchsuchen dieser Ressourcen keine Abhilfe schafft, wenden Sie sich bitte an Ihren Vertragshändler oder direkt an die nächste Norman-Niederlassung.

Kontakt

Auf dieser Seite finden Sie Telefonnummern und Adressen, über die Sie sich an Ihre zuständige Norman-Niederlassung wenden können. Diese Informationen finden Sie auch auf der letzten Seite des vorliegenden Dokuments.

Copyright © 1990-2010 Norman ASA

Automatische Reparatur

Wenn bei der installierten Version der Security Suite Probleme auftreten, können Sie jederzeit probehalber eine automatische Reparatur durchführen lassen, bevor Sie sich an den Kundendienst wenden.

Wenn Sie auf **Automatische Reparatur** klicken, wird im Hintergrund ein Vorgang gestartet, bei dem Ihre Installation geprüft und ggf. Dateien oder Komponenten aktualisiert werden. Während der Durchführung der automatischen Reparatur wird im Taskleistenmenü das Zahnsymbol angezeigt. Eine Erläuterung der Taskleistensymbole, die für die Security Suite von Bedeutung sind, finden Sie auf Seite 14.

Wenn Sie keinen Zugriff auf die Benutzeroberfläche haben, können Sie über `c:\Programme\Norman\nvc\bin` die Datei `delnvc5.exe` starten und die Option **Reparieren** wählen.

Protokollanzeige

Hierbei handelt es sich um eine Funktion, die die Anwendung überwacht und diverse Informationen zu Benachrichtigungen anzeigt, darunter Typ, Ursprung, Uhrzeit und Datum, Anwendung und Details.

Copyright © 1990-2010 Norman ASA

NSS deinstallieren

Es gibt zwei Methoden, Norman Security Suite zu deinstallieren. Eine verwendet die Windows-Funktion **Programme hinzufügen/entfernen**. Die andere verwendet das Deinstallationsprogramm von Norman.

1. Verfahren Sie folgendermaßen, wenn Sie über das Windows-Betriebssystem vorgehen möchten:
   - Gehen Sie nacheinander auf **Start > Systemsteuerung > Programme hinzufügen/entfernen**.
     - Wählen Sie unter Vista **Programme und Funktionen**.
   - Führen Sie einen Bildlauf bis zur Anwendung „Norman“ aus, und markieren Sie diese.
   - Wählen Sie die Option **Entfernen**.
     - Nach der Deinstallation des Programms starten Sie den Computer neu.

2. Verfahren Sie folgendermaßen, wenn Sie das Deinstallationsprogramm von Norman verwenden möchten:
   - Gehen Sie nacheinander auf **Start > Ausführen**, und geben Sie den Dateipfad zu `delnvc5.exe` ein.
     - Der Standardpfad lautet `C:\Programme\Norman\nvc\bin\delnvc5.exe`.
   - Wählen Sie die Option **Entfernen**.
     - Führen Sie nach entsprechender Aufforderung einen Neustart des Computers durch.

Copyright © 1990-2010 Norman ASA

Anhang A

Was ist eine Sandbox?

Als Sandbox wird die Technik bezeichnet, mit der eine Datei auf unbekannte Viren untersucht wird. Der Name wurde bewusst gewählt, denn das Verfahren lässt zu, dass nicht vertrauenswürdiger, möglicherweise mit Viren infizierter Code auf dem Computer ausgeführt wird – allerdings nicht auf dem realen Compter, sondern in einem simulierten und abgegrenzten Bereich. Die Sandbox enthält alles, was ein Virus auf einem realen Computer erwartet. Auf diesem „Spielplatz“ kann sich der Virus replizieren, ohne Schaden anzurichten. Jeder Schritt wird überwacht und protokolliert. In der Sandbox wird der Virus entlarvt. Da alle seine Aktionen aufgezeichnet werden, kann automatisch ein Gegenmittel für diesen neuen Eindringling erzeugt werden.

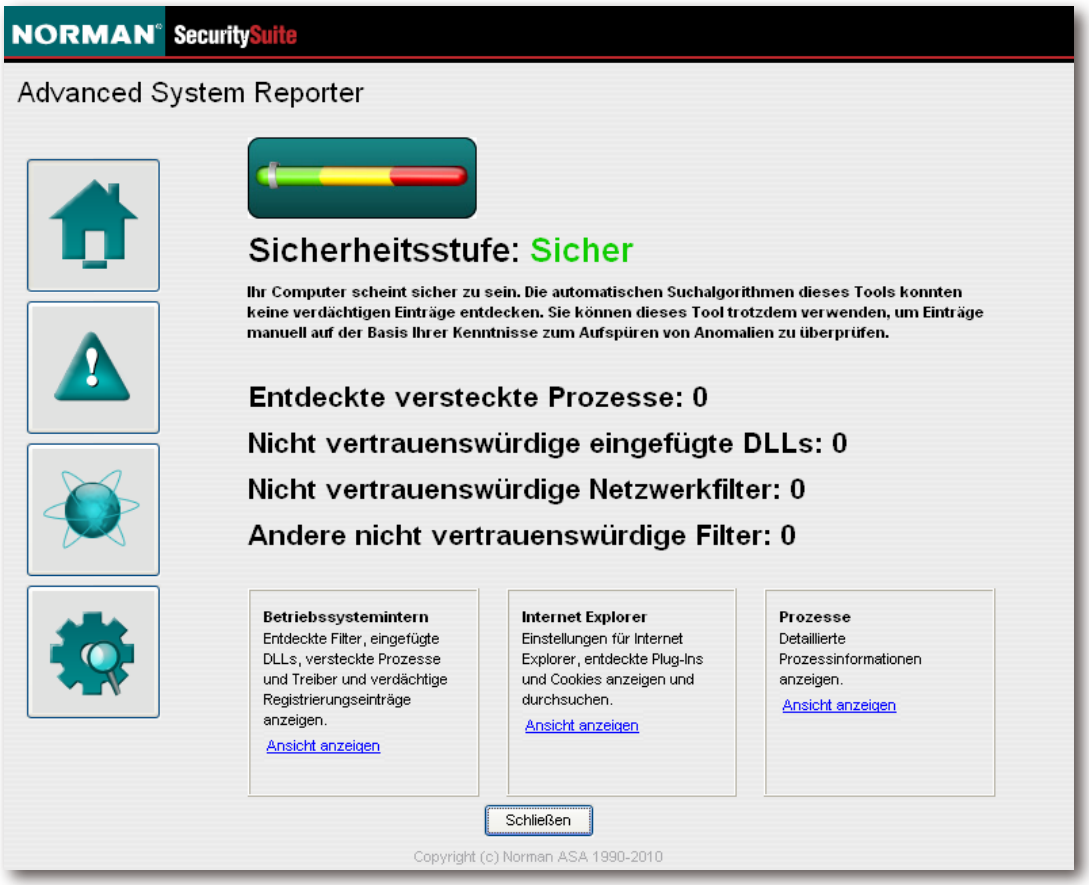
Ein moderner E-Mail-Wurm kann innerhalb von Sekunden Zehntausende von Workstations infizieren. Die Sandbox-Funktion von Norman kann sich als wertvolles Werkzeug für das „Einfangen“ neuen zerstörerischen Codes erweisen.

Copyright © 1990-2010 Norman ASA

Anhang B

Advanced System Reporter

Dieses Werkzeug ist für erfahrene Benutzer gedacht. Es erkennt unbekannte Spyware und Rootkits, indem es Ihren Computer nach ungewöhnlichen Vorgängen absucht. Verdächtige Einträge, z. B. verdeckte Prozesse, unbekannte Autostart-Prozesse, unbekannte Systemfilter usw. könnten auf bösartige Anwendungen verweisen.


NORMAN SecuritySuite
Advanced System Reporter
Sicherheitsstufe: Sicher
Ihr Computer scheint sicher zu sein. Die automatischen Suchalgorithmen dieses Tools konnten keine verdächtigen Einträge entdecken. Sie können dieses Tool trotzdem verwenden, um Einträge manuell auf der Basis Ihrer Kenntnisse zum Aufspüren von Anomalien zu überprüfen.
Entdeckte versteckte Prozesse: 0
Nicht vertrauenswürdige eingefügte DLLs: 0
Nicht vertrauenswürdige Netzwerkfilter: 0
Andere nicht vertrauenswürdige Filter: 0
Betriebssystemintern
Entdeckte Filter, eingefügte DLLs, versteckte Prozesse und Treiber und verdächtige Registrierungseinträge anzeigen.
Ansicht anzeigen
Internet Explorer
Einstellungen für Internet Explorer, entdeckte Plug-Ins und Cookies anzeigen und durchsuchen.
Ansicht anzeigen
Prozesse
Detaillierte Prozessinformationen anzeigen.
Ansicht anzeigen
Schließen
Copyright (c) Norman ASA 1990-2010

Betriebssystemintern

Hiermit könnten Sie Details zu verdeckten Prozessen und Treibern, Registrierungseinträgen, installierten Filtern und eingefügten DLLs einsehen und bearbeiten.

Internet Explorer auswählen

Hiermit können Sie Details zu Einstellungen, Plug-ins und Cookies einsehen und bearbeiten.

Prozesse

Hiermit können Sie Details zu Autostart, Diensten und anderen Prozessen einsehen und bearbeiten.

Auch wenn sich erfahrenen Benutzern diese Optionen vermutlich von selbst erschließen, können Sie Informationen zu diversen Themen abrufen, indem Sie im unteren Bereich des Dialogfelds Advanced System Reporter auf die Option **Was ist ...?** klicken.

Copyright © 1990-2010 Norman ASA

Betriebssystemintern

Versteckte Prozesse

Ein versteckter Prozess ist im Benutzermodus nicht sichtbar, auch wenn er aktuell auf dem Computer ausgeführt wird. Wenn ein Prozess im Benutzermodus versteckt wird, wurde er durch einen „Rootkit" versteckt. Meist handelt es sich um einen Treiber, der einen bösartigen Prozess für den Benutzermodus versteckt, damit Standard-Antivirensoftware ihn nicht erkennt.

Wenn Sie einen versteckten Prozess auf Ihrem Computer haben, ist es wahrscheinlich, dass dieses Dienstprogramm auch mindestens einen verdächtigen Eintrag in der Kategorie „Installierte Filter" platziert hat. Bei diesen Einträgen handelt es sich um den Rootkit selbst.

Registrierungseinträge

Die Registrierung interpretiert Dinge unterschiedlich im Benutzer- und im Kernel-Modus. Dies bedeutet, dass manche Verfahren Registrierungseinträge vor Antivirenanwendungen im Benutzermodus verdecken. Registrierungseinträge, die solchen Verfahren entsprechen, gelten als verdächtig.

Installierte Filter

Filter sind Treiber oder DLLs, die in eine Anwendung eingefügt werden und Daten verändern können, bevor diese eine Anwendung erreichen.

- **LSP (Layered Service Provider)**
  Ein LSP ist ein Netzwerkfilter, der in alle Anwendungen geladen wird, wenn diese WinSock laden, die allgemeine Methode für Anwendungen, um auf das Netzwerk zuzugreifen. Solche Netzwerkfilter können den Datenverkehr Ihres Computers im Netzwerk in beiden Richtungen verändern und blockieren. Diese Technik wird oft von Personal Firewalls und Produkten für den Kinder- und Jugendschutz verwendet.
  Bösartige Netzwerkfilter können Suchergebnisse verfälschen, Ihren Netzwerkdatenverkehr ausspähen, unerwünschte Werbung anzeigen und Sie zu schädlichen Websites umleiten.
- **SSDT (System Service Dispatch Table)**
  Dies ist ein Spezialtreiber, der die SSDT verändert, um Operationen filtern zu können, die von allen Anwendungen ausgeführt werden, z. B. das Öffnen oder Lesen einer Datei oder das Starten einer neuen Anwendung. Er wird oft von Sicherheitsanbietern verwendet, um Schadsoftware daran zu hindern, schädliche Änderungen an Ihrem Computer vorzunehmen.
  Ein schädlicher SSDT-Treiber kann jedoch enorme Rootkit-Fähigkeiten erlangen. Wenn Sie einen unbekannten SSDT-Treiber auf Ihrem Computer haben und außerdem einen oder mehrere verdeckte Prozesse, dann ist die Wahrscheinlichkeit eines vorhandenen Rootkits sehr hoch.

Eingefügte DLLs

Eine DLL ist ein Programmmodul, das in einer separaten Datei gespeichert wird, damit mehrere Anwendungen es gemeinsam nutzen können oder um Erweiterungen für vorhandene Anwendungen bereitzustellen. Eine DLL wird von der Anwendung geladen, sobald sie benötigt wird.

- **Eingefügte DLL**
  Es ist möglich, eine Anwendung dazu zu zwingen, eine DLL eines Drittanbieters zu laden. Das geschieht, selbst wenn der Anbieter der Anwendung dies nicht beabsichtigt hat und die DLL nicht explizit geladen wird. Das ist eine weit verbreitete Technik für Malware, da das Code-Modul innerhalb der DLL die vollständige Kontrolle über die Anwendung übernehmen kann. Ferner kann es Operationen im Namen der Anwendung ausführen und damit dem Betriebssystem und der Sicherheitssoftware vorgaukeln, dass die Anwendung selbst die Operation ausgeführt hat.
  Es gibt einige wenige legitime Anwendungsfälle für den Einsatz eingefügter DLLs in anderen Anwendungen, z. B. für das Debuggen einer Anwendung, wenn diese abgestürzt ist. Im Allgemeinen kann jedoch davon ausgegangen werden, dass eine Anwendung, die DLLs in andere Anwendungen einfügt, entweder schlecht konzipiert oder bösartig ist.
  Sie sollten besondere Vorsicht walten lassen, wenn Sie eingefügte DLLs in Ihrem System finden. Jede DLL, die nicht von einem ganz und gar vertrauenswürdigen Anbieter stammt, sollte entfernt werden. Sogar die Software, die Sie selbst aus dem Internet geladen und installiert haben, könnte in Wirklichkeit ein Trojaner sein.

Versteckte Treiber

Ein versteckter Treiber ist im Benutzermodus nicht sichtbar, obwohl er gerade auf dem Computer ausgeführt wird. Ein Treiber, der im Benutzermodus versteckt ist, besitzt Rootkit-Funktionalität. Der Treiber versteckt auf der Festplatte seine Dateien, seine Registrierungseinträge oder seinen Speicherplatz.

Copyright © 1990-2010 Norman ASA

Internet Explorer

Einstellungen
Anzeigen und Bearbeiten der Einstellungen für den Microsoft Internet Explorer.

Plug-ins
Ein Plug-in für Browser bietet zusätzliche Funktionen, z. B. Symbolleisten oder Suchverbesserungen, aber es kann auch unerwünschte Werbung verursachen und sogar Ihr Surfverhalten und Ihre Kennwörter ausspionieren.

- **Browser Helper-Objekt**
  - Ein Browser Helper-Objekt (BHO) ist ein Plug-in für den Internet Explorer, das dazu gedacht ist, eingehenden oder ausgehenden Datenverkehr Ihres Browsers zu verändern. Diese Art von Plug-in wird am häufigsten von Spyware-Anwendungen verwendet, weil es alle Daten, die an und von Ihrem Browser kommen, einfach erfassen kann.
- **Symbolleiste**
  - Eine Symbolleiste ist ein Plug-in für den Internet Explorer, das neue Einträge im Symbolleistenbereich des Browsers erstellt. Diese Art von Plug-in kann von Adware verwendet werden, um Werbung anzuzeigen.
- **URL-Sucheingriffe**
  - Ein Sucheingriff ist dazu gedacht, eingegebene Webadressen umzuleiten, und er kann dabei helfen, falsch oder unvollständig eingegebene Adressen richtig aufzulösen. Beispielsweise wird „norman.com“ standardmäßig in „http://www.norman.com“ übersetzt. Diese Art von Plug-in kann von Adware-Anwendungen verwendet werden, um Sie auf andere Websites umzuleiten.
- **Andere**
  - Andere Plug-ins können dem Browser Menüoptionen oder Benutzerbedienfelder hinzufügen. Diese Art von Plug-in kann von Adware verwendet werden, um Werbung anzuzeigen.

HINWEIS: Alle Plug-ins sind technisch in der Lage, den Datenverkehr zu verändern und Benutzerdaten auszuspähen, auch wenn das entsprechende Plug-in nicht für diesen Zweck konzipiert wurde.

Cookies
Ein Cookie ist eine kleine Datei, die im Ordner für temporäre Internetdateien gespeichert wird, weil Sie die zugehörige Webseite besucht haben.

- **Missverständnisse**
  - Ein gängiges Missverständnis ist, dass Cookies schädlich sind, dass sie Popups und unerwünschte Werbung erzeugen und dass sie Ihren Computer schädigen können. Einige Anti-Spyware-Anbieter führen sie sogar als Spyware auf und erzeugen bei bestimmten Cookies Alarmmeldungen (speziell bei den sogenannten „Tracking Cookies“).
  - Cookies sind NICHT GEFÄHRLICH und können Ihren Computer nicht schädigen. Die in dieser Ansicht angezeigten Cookies bergen daher kein Risiko. Sie können sie allerdings nach Wunsch löschen.
- **Der Zweck von Cookies**
  - Cookies werden von Webservern verwendet, um Benutzer unterscheiden und Daten auch über mehrere Besuche hinweg beibehalten zu können. Durch das Löschen eines Cookies gehen daher Benutzereinstellungen, Inhalte von Einkaufswagen und Anmeldedaten verloren, und zwar von allen zurückliegenden Besuchen. Sie müssen sich daher beim nächsten Besuch u. a. neu anmelden.
- **Tracking Cookies**
  - Manche Websites verwenden Cookies von Drittanbietern, um Ihre Bewegungen zwischen Websites zu verfolgen. Manche Menschen empfinden dies als Einbruch in die Privatsphäre. Die von Ihnen besuchten Webserver können diese Kommunikation über Websites hinweg allerdings auch direkt bewerkstelligen, ohne dafür auf Tracking Cookies angewiesen zu sein.
  - Unser Tool unterscheidet nicht zwischen den sogenannten „Tracking Cookies“ und „normalen“ Cookies, da der einzige Unterschied darin besteht, dass Tracking Cookies von einem Drittanbieter verwaltet werden. Vom Standpunkt der Malware-Bekämpfung ist das kein großer Unterschied.

Copyright © 1990-2010 Norman ASA

Prozesse

Autostart

Eine auf Ihrem Computer installierte Anwendung – egal ob legitim oder bösartig – wird meist versuchen, automatisch zu starten, sobald der Computer hochfährt. Ein Programm, das automatisch zu starten versucht, kann das Betriebssystem anweisen, automatisch mit den gleichen Rechten wie der aktuelle Benutzer zu starten, wenn der Computer hochfährt. Oder es kann einen Hintergrunddienst installieren, der mit erhöhten Zugriffsrechten ausgeführt wird. Eine Angriffsverteidigungsanwendung kann Zugriffsversuche dieser Art verhindern.

HINWEIS: Die Autostart-Funktion deckt nicht die Autorun-Funktion für CDs oder USB-Sticks ab.

Dienste

Ein Dienst ist ein Hintergrundprozess, der jedes Mal gestartet wird, wenn der Computer hochfährt. Dies ist ein normales Verhalten.

Copyright © 1990-2010 Norman ASA

Niederlassungen von Norman

Dänemark
Norman Data Defense Systems AS
Blangstedgårdsvej 1,
DK-5220 Odense SØ
Tel: +45 63 11 05 08
Fax: +45 65 90 51 02
E-Mail: info@normandk.com
Web: www.norman.com/dk

Deutschland
Norman Data Defense Systems GmbH
Zentrale, Gladbecker Str. 3,
D-40472 Düsseldorf
Tel: +49 0211 5 86 99-0
Fax: +49 0211 5 86 99-150
E-Mail: info@norman.de
Web: www.norman.com/de

España
Norman Data Defense Systems
Camino Cerro de los Gamos 1, Edif.1,
28224 Pozuelo de Alarcón MADRID
Tel: +34 91 790 11 31
Fax: +34 91 790 11 12
E-Mail: norman@normandata.es
Web: www.norman.com/es

France
Norman France
8 Rue de Berri,
F-75008 Paris
Tel: +33 1 42 99 94 14
Fax: +33 1 42 99 95 01
E-Mail: info@norman.fr
Web: www.norman.com/fr

Italia
Norman Data Defense Systems
Centro Cassina Plaza,
Via Roma, 108
20060 Cassina de'Pecchi (MI)
Tel: +39 02 951 58 952
Fax: +39 02 951 38 270
E-Mail: info@normanit.com
Web: www.norman.com/it

Nederland
Norman SHARK B.V.
Postbus 159,
2130 AD Hoofddorp
Tel: +31 23 789 02 22
Fax: +31 23 561 31 65
E-Mail: support@norman.nl
Web: www.norman.com/nl

Norge
Norman ASA
Headquarter and Sales Norway
Hovedkontor og salg Norge
Hausanschrift: Strandveien 37, Lysaker
Postanschrift: PO Box 43, N-1324
Lysaker
Tel: +47 67 10 97 00
Fax: +47 67 58 99 40
E-Mail: norman@norman.no
Web: www.norman.com/no

Schweiz/Suisse/Svizzera
Norman Data Defense Systems AG
Münchensteinerstraße 43
CH-4052 Basel
Tel: +41 61 317 25 25
Fax: +41 61 317 25 26
E-Mail: norman@norman.ch
Web: www.norman.com/ch

Sverige
Norman Data Defense Systems AB
Södra Grytsgatan 7, 2tr,
Norrköping Science Park
S-602 33 Norrköping
Tel: +46 11 230 330
Fax: +46 11 230 349
E-Mail: sales.se@norman.com
Web: www.norman.com/se

United Kingdom
Norman Data Defense Systems (UK) Ltd
Exchange House,
494 Midsummer Boulevard
Central Milton Keynes,
MK9 2EA
Tel. 1: +44 08 707 448 044
Tel. 2: +44 01 908 255 990
Fax: +44 08 701 202 901
E-Mail: info@normanuk.com
Web: www.norman.com/en-uk

United States
Norman Data Defense Systems Inc.
9302 Lee Highway,
Suite 950A,
Fairfax, Virginia 22031
Tel: +1 703 267 6109
Fax: +1 703 934 6368
E-Mail: norman@norman.com
Web: www.norman.com/en-us

Norman ASA ist ein weltweit führender Anbieter von Datensicherheitslösungen, Internetschutz und Analysetools. Mit seiner Sandbox-Technologie bietet Norman einzigartigen offensiven Schutz, der effektiver als alle vergleichbaren Lösungen ist. Neben der Schwerpunktsetzung auf offensiver Antivirentechnologie bietet Norman auf Grundlage entsprechender Allianzen eine ganze Bandbreite an Datensicherheitslösungen an.

Norman wurde im Jahr 1984 gegründet und hat seinen Unternehmenssitz in Norwegen. Wichtigste Märkte sind Kontinentaleuropa, Großbritannien und USA.

Copyright © 1990-2010 Norman ASA

NORMAN®